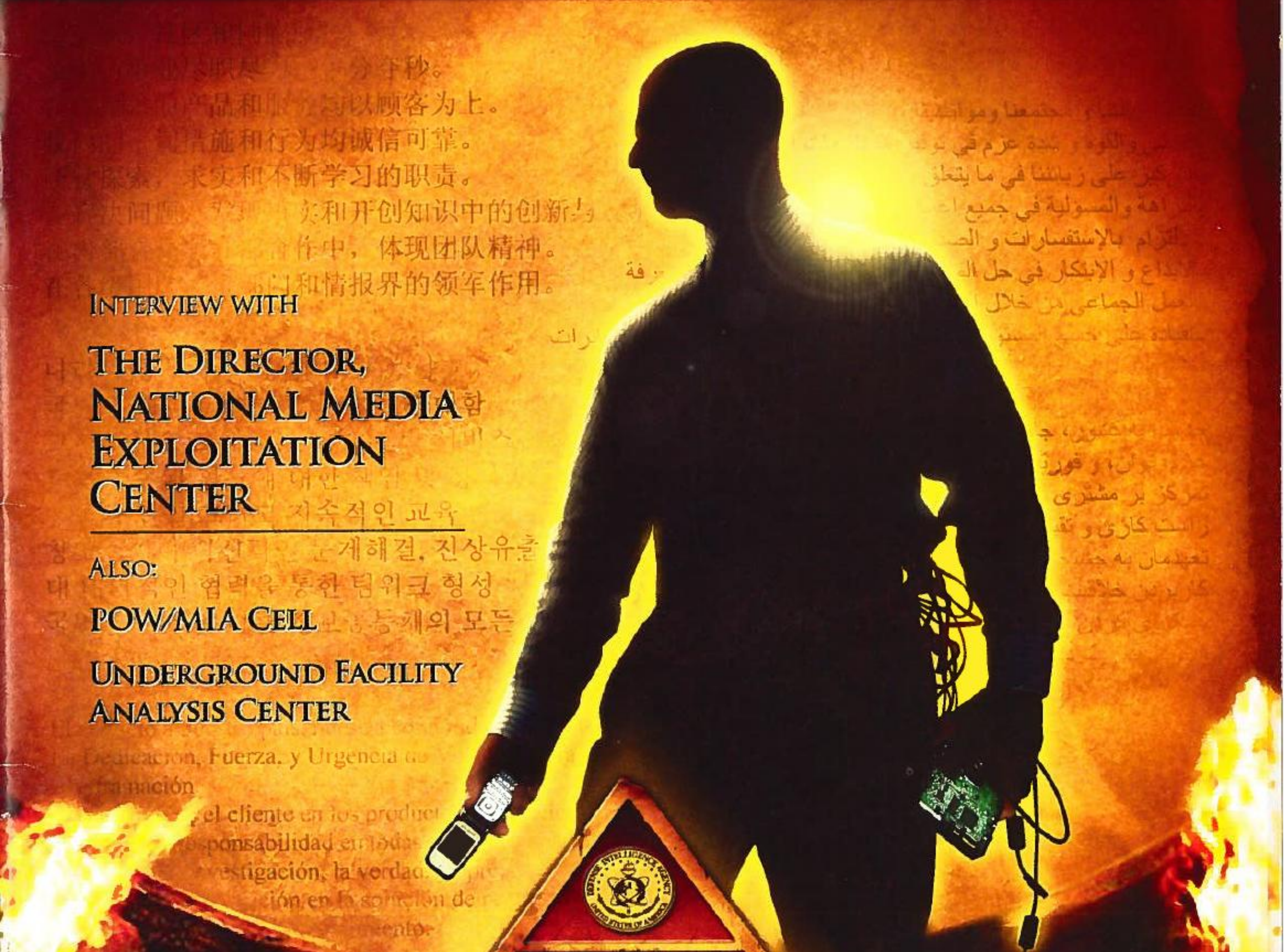
COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

COMMUNIQUÉ

MAY/JUNE 2010

A DEFENSE INTELLIGENCE AGENCY PUBLICATION


以顾客为上。
措施和行为均诚信可靠。
求实和不断学习的职责。
和开创知识中的创新
体现团队精神。
情报界的领军作用。
지속적인 교육
Dedicación, Fuerza, y Urgencia
el cliente en los produc
responsabilidad en toda
investigación, la verdad

INTERVIEW WITH

THE DIRECTOR, NATIONAL MEDIA EXPLOITATION CENTER

ALSO:

POW/MIA CELL

UNDERGROUND FACILITY ANALYSIS CENTER

NATIONAL CENTERS

THE DEFENSE INTELLIGENCE AGENCY IS THE EXECUTIVE AGENT FOR SEVERAL NATIONAL CENTERS WITH MISSIONS SPANNING THE GLOBE. THESE CENTERS SOLVE TODAY'S CRITICAL INTELLIGENCE CHALLENGES, AND THEIR IMPACT CAN BE FELT AT HOME AND ON THE FRONT LINE.

MAY/JUNE 2010 • Volume 23/Number 4
COMMUNIQUÉ
A Defense Intelligence Agency Publication

LTG Ronald L. Burgess Jr.
Director, DIA

Letitia "Tish" Long
Deputy Director, DIA

Donald L. Black
Chief, Public Affairs

Jane A. McGehee
Chief, Internal Communications

Dana M. Black
Managing Editor

Margan C. Kerwin
Jennifer M. Redding
Kate S. Worley
Editorial Staff

Brian D. Nickey
Design/Layout

Graphic Design and Publishing Services Branch
Printing and Posting

DIA's Communiqué is an authorized agency information publication, published for employees of DIA and members of the defense intelligence community. Contents of the Communiqué are not necessarily the official views of, or endorsed by, the U.S. government or the Department of Defense. Articles are edited for style, content and length. Correspondence should be addressed to: DIA Communiqué, Public Affairs Office, 200 MacDill Blvd., Bolling Air Force Base, Washington, D.C., 20340. Telephone: 202-231-0814 (DSN: 428-0814). The DIA Public Affairs Office welcomes your comments, which may be e-mailed to our Internet address at DIA-PAO@dia.mil or to our JWICS e-mail address at diem908-DIA@dodiis.ic.gov.

www.dia.mil

Article Submission Deadlines

July/Aug. 2010 issue — June 2, 2010
Year in the Life 2010 issue — Aug. 4, 2010

may/june 2010

HEADLINES

A Survivor's Story 2
By SSG Chris A. Suter, DH

DIA Greening Council Launches 4
By Dr. Daneta G. Billau, DA

AFRICOM's Unique Mission Yields SERENGETI-KD 4
By LTC Enrique Camacho and Bari A. Lee, AFRICOM

Simulating Success 6
By Russell J. Spaulding, HC

Protecting You Against Terrorism 7
By Andrew E. Lenze, DA

Unofficial Foreign Contact Reporting 9
By Victor R. Bryant and Dr. Daneta G. Billau, DA

Capturing Hearts and Minds 10
By Adrian "Zeke" Wolfberg, CS

Protecting Critical Defense Infrastructure One Partnership at a Time 12
By Kristopher C. McQueen, DDC

Command Training Facility 'Punches Above Its Weight' 13
By Peter G. Park, EUCOM

Teaching Iraqis to Teach Iraqis 14
By Maj Rich "Checker" Greenslit, HC

SITCEN Keeps Leaders in the Know 16
By Scott K. Muessig, DA

Detachment of the Month: Force Protection Detachment SOFIA 17
By the Force Protection Detachment Staff, DX

2010 IC Collection Assessments Conference 19
By Jacob Ulvila, NIC-C, and John R. Jones, DJ

EXECUTIVE VISION

Interview with Bill Mills, Director of the National Media Exploitation Center 20
By the Communiqué Staff, CP

NATIONAL CENTERS

Making Media Exploitation More Efficient 21
By Terry S. McCall, NM

NMEC: Technical Exploitation of Digital Media 22
By Tammy Poor, NM

NEXSYS: The Next Generation Architecture 24
By Caryn D. Mercadante, NM

DOMEX Ops Keeps it REAL 26
By Colleen M. Foster, NM

Creating DOMEX Professionals 26
By Trevor G. Hassett, NM

Bringing DOMEX Capability to Our Coalition Partners 27
By Trevor G. Hassett, NM

DOMEX Enterprise Governance and Doctrine 28
By Dave Barkley, NM

UFAC Digs Deep to Find Covert Facilities 29
By the Underground Facility Analysis Center, DI

Cell Helps Bring Missing Service Members Home 30
By the IC Prisoner of War/Missing In Action Analytic Cell, DI

Medical Intelligence Relies on Teamwork 32
By Damien K., NGA

⁖LEADING EDGE

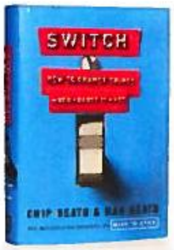
Unlocking the Mystery of PKI 33
By Juanita L. Hairston, DS

⁖COMMUNITY OUTREACH 34

⁖PHOTO OP 36

30

29



10

7

34

A SURVIVOR'S Story

By SSG Chris A. Suter, DH

People around the world felt the repercussions of the Jan. 12 earthquake that struck Port-au-Prince, Haiti, but few felt it the same way as DH's SSG Chris Suter. This is the story of how he survived the devastating quake and the community that rallied around him.

Tuesday, Jan. 12, was a typical day. I had gotten home from work and was turning on my personal computer. As the computer started up, I began to hear a roar all around me, which reminded me of being under attack in Iraq.

My house began to violently shake. As I ran out of my office, bouncing off the walls into the hallway, I saw a picture of my oldest son, Josh, falling off the wall in slow motion. As I braced myself between the walls, trying to get to my front door, I remember the floor dropping out from under me. The last thing I remember was my head hitting the ceiling. Ironically, I didn't feel fear at this point as the events were happening so quickly.

My guess is that I was unconscious for about five minutes or so after the earthquake. When I woke up, my left leg was pinned under a door and my body was positioned at an unnatural angle in the rubble. My house had literally crumbled to the ground with me in it. About that time, the first aftershock hit, which I later determined was seven minutes after the main earthquake.

I estimate that I was trapped for approximately 30 minutes before help arrived. After assisting my civilian neighbors downstairs, a U.S. Coast Guard commander and neighbor arrived with help and pulled the door and concrete off of my leg. With support, I walked to the street in front of my house where a blanket was laid out for me to lie down on. To my surprise, there were at least 30 Haitians gathered in front of my driveway helping the injured. Of the four individuals that lived in my building complex, three of us were trapped in the rubble.

SSG Chris Suter

As I lay there waiting for a vehicle to arrive, I learned that all roads up to my home had been blocked by earthquake debris — cinder blocks, walls, trees,

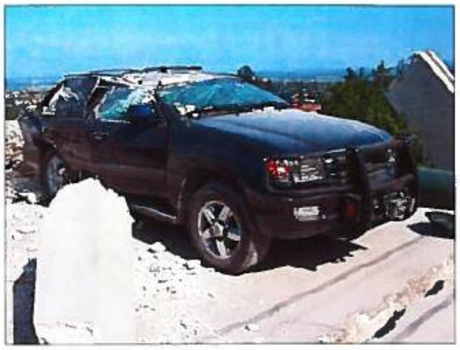
"My house began to violently shake. As I ran out of my office, bouncing off the walls into the hallway, I saw a picture of my oldest son, Josh, falling off the wall in slow motion."

etc. It took just over four hours to assemble enough embassy employees to carry three injured personnel (myself included) past the road blocks and down the hill. One of my neighbors was carried out on a ladder; another neighbor was carried out on a board. I was carried out on a steel grate that probably weighed as much as I did. There weren't enough rescuers to carry the three injured so they started taking us down in relays.

Being carried down my street past my Haitian neighbors' newly formed piles of rubble was such an unreal experience. With no place to go, Haitians filled every open area imaginable. Most were praying; many were huddled in small groups. As these people noticed the stretcher being carried by, they came to help. It took eight men to carry my stretcher; seven of these were my neighbors who had just lost everything. In total, I was carried about two miles.

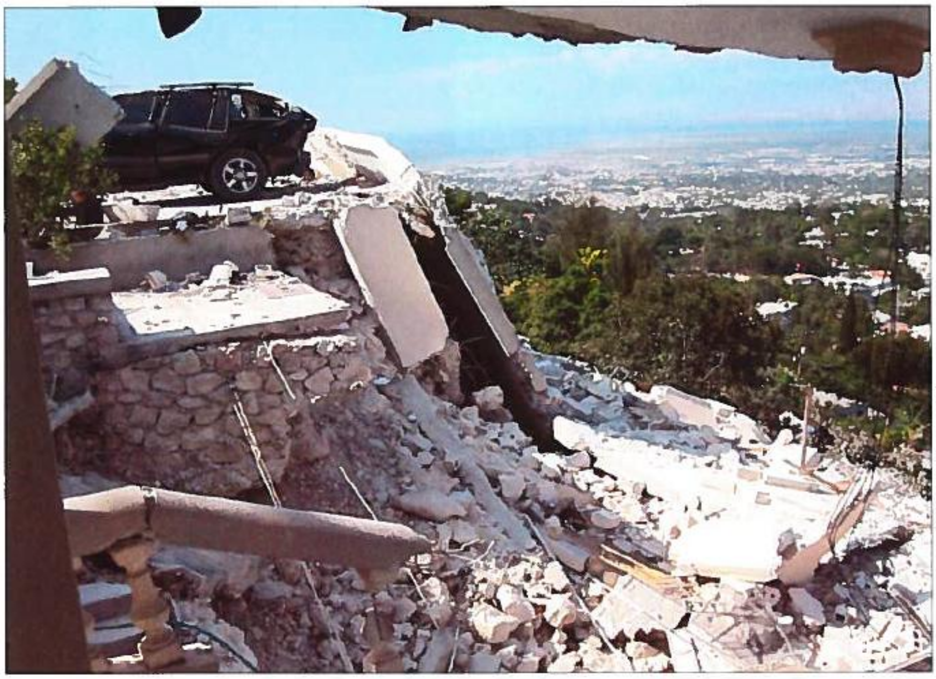
At one point in my trip down the mountain, the road became so narrow that I had to be carried on the edge of cliff that appeared to have a 100 foot drop off! There wasn't enough room to carry the litter on either side; there was only room on the path for a couple of men at my head and toe. As I looked to my left, all I could see was a very long drop and the four guys carrying me, struggling hard to manage me as they stepped over the rubble underfoot.

Eventually, we reached a vehicle and were taken to a small, minor emergency medical clinic. There wasn't a waiting room or a treatment room. I found a spot on the floor out of the way, and was given a shot for the pain.



◄ SSG Chris Suter's car was destroyed during the January earthquake in Haiti.

SSG Chris Suter was trapped inside his home, pictured here, during the January earthquake in Haiti. He along with three of his neighbors had to be rescued from the rubble. ▼



Photos courtesy of Chris A. Suter, DH

My neighbor Emily was a tremendous source of support throughout the night. She stayed with the three of us at the emergency clinic making sure we were comfortable, giving us water, and at times shooing away gawkers with cell phone cameras. Emily took time to chat with me, keeping my morale up and my spirits high, and I can't imagine living through that night without her.

At first light, we were transported by a Coast Guard rescue helicopter to the naval hospital in Guantanamo Bay, Cuba, for triage treatment before our final destination in Miami. While in Guantanamo Bay, X-rays revealed I had suffered a broken leg, eight broken ribs and a punctured lung.

Shortly after, I was flown to Jackson Memorial Hospital in Miami. X-rays confirmed that seven of my ribs were broken in two places; three of those were broken three or more times. With the tremendous care and support from the staff at Jackson Memorial, I was released from the hospital Jan. 22.

The memories of those 10 days will remain with me for a very long time.

Editor's Note: SSG Chris Suter is the OPSNCO at U.S. Defense Attaché Office Port-au-Prince, Haiti. He arrived on station Dec. 1, 2009, six weeks before the earthquake. He is working in the Latin American Division (DHO-5) at the DIAC while recovering from his injuries.

DIA Greening Council LAUNCHES

By Dr. Daneta G. Billau, DA

DIA's new Greening Council is made up of people like you to promote greening at work and at home.

Photo by John O'Connor, Toeffler Associates

DIA Greening Council members, pictured from left to right: Wendy Johnson, Margan Kerwin, David Sheets, Daneta Billau, Mika Cross, Doug Vibbert, Kelly Lael, Jesse Fairall, Susan Sternad-Basel, James Manzelmann, Renee Robinson, and Lora Conk. VTC members not pictured include Deborah Keimig, Lynn McNamee and Nancy Roemer.

The Directorate for Mission Services (DA) launched the DIA Greening Council Feb. 18. Deputy Director for Mission Services James Manzelmann, the council's senior sponsor, hosted the meeting with 20 volunteers from across the agency who want to make a difference. The council is chartered to promote greening within the work force at DIA to magnify efforts toward achieving challenging federal mandates for a green government.

At the initial meeting, council members quickly formed a consensus to implement "Green Fridays" this summer at DIA. Council members are preparing an information campaign about important greening topics to encourage employees to take environmentally conscious measures, such as reduce energy and water use; purchase green products like Energy Star equipment; and use green supplies and materials whenever possible. The DIA Greening Council promotes ways employees can help DIA go green, like increasing recycling; turning off lights when they are not needed; making sure fans and other equipment are powered down when not in use; maintaining steady thermostat temperatures; and using duplex print functions, recycled paper and draft print functions for draft documentation.

Employee participation in greening DIA around the world is a critical ingredient in solutions to help DIA meet tough greening milestones, with the added benefit of saving DIA hundreds of thousands of dollars in utility bills, wasted supplies and waste management. The DIA Greening Council is energized and already in motion preparing for Green Fridays this summer. Anyone can join the council by contacting Dr. Daneta Billau at (703) 907-4694. Meetings are held monthly with video teleconferencing around the world.

Welcome to a greener DIA!

Visit the InterComm newsletter for regular articles from the Greening Council.

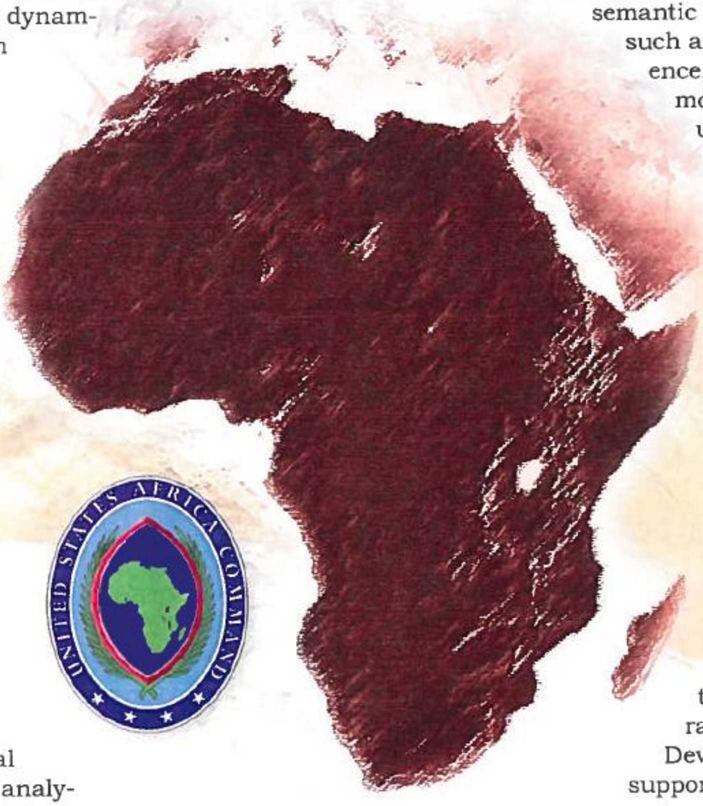
AFRICOM's Unique Mission Yields SERENGETI-KD

By LTC Enrique Camacho and Bari A. Lee, AFRICOM

AFRICOM's unique mission and fresh start allowed intel designers to create a digital architecture that is unparalleled for any other command — and they want input from you.

U.S. Africa Command (AFRICOM) is the first geographic combatant command purposefully designed from the ground up, unencumbered by legacy systems and architectures. As such, the philosophy embraced by the founders focused on "the data" and tools, which are primarily mission or problem focused, and commodity products that will change over time. This fresh outlook afforded AFRICOM intel designers the maximum

> **"SERENGETI-KD provides the command an analytical lab environment where analysts can test hypotheses and experiment with different analytic techniques."**



flexibility to experiment with architectures, methods and ideas.

Throughout 2008 and early 2009, AFRICOM's draftsmen tested concepts dealing with data deficiencies and partnered with multiple organizations within the intelligence community (IC), Department of Defense (DOD) and academia to test assumptions and validate architectures. The result of these experiments produced a program titled SERENGETI-KD, or Special Environment Related to Non-traditional Geospatial Environmental Topography Intelligence-Knowledge Development. The program's goals center on two key themes: First, to put into operation socio-cultural dynamics to understand the human terrain in areas where the command has operational elements or activities. Second, to design a technical architecture that supports the analytic environment.

The foundation of SERENGETI-KD relies on an aggressive data-first mentality. To that end, AFRICOM implemented this digital architecture that is specifically engineered to produce non-traditional geospatial, environmental, topography intelligence and knowledge development-oriented intelligence products. This SERENGETI-KD hardware and software architecture provides an unprecedented socio-cultural production capability to the analysis within AFRICOM's Knowledge Development Division. SERENGETI-KD enables the discovery, storage and management of Africa-centric data sets unconstrained by file type or size. This unique design comprises advanced automated data harvesters, multi-lingual translators, data managers and storage systems that operate in near-full automation to provide analysis of emerging events vis-à-vis visual alerts and customized trackers across multiple domains. Coordinating 16 software vendors on more than 20 digital servers across multiple domains, SERENGETI-KD is AFRICOM's test bed for innovative ways to acquire, ingest, store, retrieve, analyze and visualize data.

Powered by a state of the art analytic environment known as "Savanna," SERENGETI-KD provides the command an analytical lab environment where analysts can test hypotheses and experiment with different analytic techniques. Being developed with the aid of AFRICOM intelligence professionals, Savanna will leverage the full digital data architecture of SERENGETI-KD and employ semantic models to represent concepts such as confidence, bias and influence, all of which are essential to modeling human behaviors and understanding cultures.

Although greatly encouraged by the initial development and success of SERENGETI-KD, AFRICOM approaches the advanced implementation of Savanna with a sober view, understanding that many have ventured down this path with high hopes only to fall short of expectations. AFRICOM therefore invites those with experience and lessons learned to assist and advise in the further development and implementation of SERENGETI-KD. Similar to the approach of Gran Prix racing teams, the Knowledge Development Division seeks to support AFRICOM's greater intelligence enterprise by developing and devising innovative ways to discover, manage, analyze and visualize intelligence for its users and export that knowledge, techniques and tools to the greater community.

If you have experiences you would like to share, please contact Bari Lee via JWICS e-mail.

SIMULATING Success

By Russell J. Spaulding, HC

The Joint Military Attaché School uses proven learning principles in their simulations so their students are prepped for success.

What have you learned lately? Was it on the job or in a classroom? Was it at your workstation or over a cup of coffee with a colleague? Many would say "all of the above." We are always learning, but how strategic are we when we consider both our formal and informal learning? DIA's learning professionals in the Office of Learning and Career Development (HCL) work to implement innovative strategies that will optimize both formal and informal learning to improve performance. Effective learning does not occur without a strategy, and no organization knows this better than HCL's Joint Military Attaché School (JMAS).

JMAS has an established record of effective teaching, evidenced by accreditation from the Council on Occupational Education and success from DIA's Attaché Training Program. Key to this success is an innovative learning strategy centered on a simulation that blends the best of formal and informal learning.

For a simulation to really work, certain research-based principles of learning need to be operating. Carnegie Mellon's Eberly Center for Teaching Excellence has distilled seven basic principles that underlie effective learning:

- Students' prior knowledge can help or hinder learning.
- How students organize knowledge influences how they learn and apply what they know.
- Students' motivation determines, directs and sustains what they do to learn.
- To develop mastery, students must acquire component skills, practice integrating them and know when to apply what they have learned.
- Goal-directed practice coupled with targeted feedback enhances the quality of students' learning.
- Students' current level of development interacts with the social, emotional and intellectual climate of the course to impact learning.
- To become self-directed learners, students must learn to monitor and adjust their approaches to learning.

A robust simulation driven by these seven principles breaks through limitations of traditional classroom lecture and discussion groups. A simulation essentially is an intensive, interactive experience in which the content and roles assumed by participants are designed to reflect what people encounter in actual work. Master of Business Administration programs have developed simulations for aspiring managers to run a private corporation in the competitive marketplace. Individuals in the defense community have participated in complex war games to train like we fight. Simulations are effective because they are realistic, interactive, compelling, structured and safe. Mistakes can be made and evaluated without causing real harm. The JMAS program is an example of a simulation that works.

JMAS trains prospective military attachés and defense attaché office (DAO) staff for duty throughout the Defense Attaché System, as well as provides appropriate voluntary training for spouses of attachés and attaché staff. The school achieves this mission by delivering knowledge and skills within an overarching simulation of a DAO in a foreign country.

Photo by Dennis B. Fowler, HC

Learning beyond the classroom: Defense attaché students practice skills during one of the many interactive events during their 13-week simulation. Here they are at the Port of Baltimore gathering information on harbor activities and infrastructure.

The JMAS simulation manifests all seven principles, especially these three:

Goal-directed practice coupled with targeted feedback enhances the quality of students' learning. The simulation provides many opportunities for feedback that explicitly relate to performance objectives. The feedback is timely, frequent and constructive in a way that allows students to incorporate it into further practice. During the simulation, any corrections to performance are provided immediately and within role by role players under the direction of the faculty.

To become self-directed learners, students must learn to monitor and adjust their approaches to learning. Every defense attaché knows that learning does not stop at graduation. The simulation enables students to become conscious of their own thinking and decision-making processes so that they continue to direct their own learning. Also known as metacognition, this ability is critical for agile problem-solving in the field. Students are given requirements that they must accomplish within the scenario. There is no single method of attaining results. Students learn to use their strengths and become aware of their weaknesses within the simulation.

Students' current level of development interacts with the social, emotional and intellectual climate of the course to impact learning. Once students complete the 13-week simulation, they have been exposed — by design — to the widest spectrum of social and emotional elements that may be encountered on the job. The entire simulation is monitored by a psychologist to ensure that no portion reinforces incorrect performance or negative learning. The stress of "mission accomplishment" is high in field grade and senior officer assignments, and the simulation leverages that stress.

Learning that has a lasting impact on mission performance is what matters most. These seven principles of learning are valuable guideposts for ensuring critical knowledge is transferred to the work environment. Viewing any learning solution from the perspective of these principles is a solid step in maintaining a strategic approach to the full spectrum of learning — from formal to informal.

PROTECTING YOU Against Terrorism

By Andrew E. Lenze, DA

Everyone plays an important role in protecting the agency — and yourself — from terrorism.

Protecting you against acts of terrorism is the agency's antiterrorism (AT) program mission. This program focuses on prevention and preparedness through deterrence, detection, defense and emergency response. It takes more than five teams to implement the program: the Directorate for Mission Services' Counterintelligence and Security Office (DA/DAC), Enterprise Operations (DA/DAE) and Engineering and Logistics (DA/DAL); facility responsible building officers (RBOs) and facility antiterrorism officers (FATOs); and you — the DIA work force.

Counterintelligence and Security Office (DAC)

DAC manages the overall program, coordinates AT planning, performs risk management, disseminates threat information, facilitates training and awareness, and is the primary provider of physical security operations. An AT team in DAC coordinates and monitors all of these antiterrorism activities. The DIA Police, a team within DAC, provides physical security to most facilities hosting agency personnel. The Global Response Team provides tailored antiterrorism support to the agency's human intelligence and other forward deployed elements.

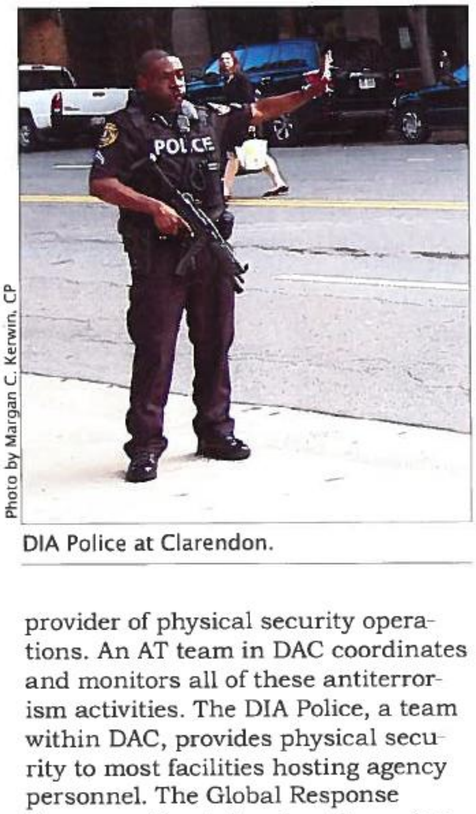


Photo by Margan C. Kerwin, CP

DIA Police at Clarendon.

Photo by Paul F. Krasley, DA

DIA's Situation Center.

Enterprise Operations (DAE)

DAE takes care of the crisis management and emergency preparedness aspects of the program. DAE's Mission Assurance team coordinates and monitors all of these activities. The Operations Readiness team supports the AT effort by providing enhanced force protection training to agency personnel deploying overseas, and Global Operations manages and monitors DIA activities throughout the world.

Engineering and Logistics (DAL)

The DAL team engineers and builds

INDIVIDUAL ANTITERRORISM RESPONSIBILITIES

- Complete annual Level I AT Awareness Training.
- Complete DIA Defensive Travel Training within 3 months prior to any travel outside the continental United States.
- Be familiar with and adhere to your facility's general security, AT and OPSEC procedures.
- Know who your responsible building occupant (RBO) and facility AT officers (FATOs) are and how to contact them.
- Prominently post a "Bomb or Other Threatening Call Checklist" and "Individual FPCON Responsibilities Card" at your workstation.
- Prominently post contact information (i.e., phone numbers and e-mail addresses) for emergency services and key personnel at your workstation.
- Remain alert to and immediately report any AT-related problems, suspicious activity or incidents.

security into our facilities. Over the years, architects and engineers have identified features that effectively and efficiently enhance protection. These features include blast resistant structures, passive and active barriers, security lighting, protected air-handling systems and mass notification systems.

RBOs and FATOs

RBOs and FATOs implement and manage the AT and physical security programs at their facilities. They perform localized risk management and AT planning, publish localized procedures, train personnel, conduct drills and exercises, and ensure suspicious activity and incident reports are promptly reported to headquarters. To identify an RBO or FATO for a particular DIA facility, check the FATO listing located on DAC's website or contact the DIA Headquarters Antiterrorism Team at (703) 907-1899 or JWICS e-mail at dise703-DIA@dodiis.ic.gov.

You

The most important element of the AT program is you, the DIA work force. It does not matter whether you are a federal employee, service member or defense contractor, or whether you are a senior executive, mid-level manager, or technician — we are all responsible for our own security as well as the protection of our co-workers, the facilities we work in, the equipment we use, and the information we process and handle each and every day.

So what are those responsibilities? They can be summed up in four actions: be informed; comply with procedures; be vigilant to the threat; and immediately report problems, suspicious activities and incidents.

Keeping yourself informed falls into three levels. First, you are required to complete your annual Level I AT Awareness Training, which provides you with an overview of terrorism, individual protective measures, terrorist surveillance techniques and methodologies, and an understanding of terrorist threat levels and force protection condition (FPCON) levels. Second, you are required to complete DIA Defensive Travel Training within three months prior to any travel outside the continental United States, which provides an overview of the current terrorist and foreign intelligence threat and reporting requirements, and informs you of any additional AT requirements placed on you by the various geographic combatant commanders. Third, you are required to know the local AT procedures for your facility and to complete any additional training required by that facility's RBO. Have you completed your annual AT awareness training? If traveling, have you completed your defensive travel training? Have you taken the time to meet your FATO and become familiar with your facility's AT procedures? For more information on travel training, go to www.dia.ic.gov/homepage/da/security/field/overseas.html.

Photo by Margan C. Kerwin, CP

It is everyone's job to sniff out something suspicious. Immediately report any unusual activity to your building's local security force, usually the DIA Police.

Complying with AT policies and procedures is the natural follow-on to keeping yourself informed. Once you know what the threat is and what your responsibilities are, you need to ensure you act accordingly. Do you have a "Bomb or Other Threatening Call Checklist" and "Individual FPCON Responsibilities Card" posted at your workstation? If not, where do we get these? Do you know how to use it? Do you know and exercise your operational security responsibilities? To obtain more information regarding antiterrorism, including visual aids or handouts, contact your FATO, or contact the DIA Headquarters Antiterrorism Team at (703) 907-1899 or JWICS e-mail at dise703-DIA@dodiis.ic.gov.

Staying alert for unusual or suspicious activities is one of the most difficult responsibilities to maintain. After a major incident, everyone is primed and ready — vigilant for anything out of the ordinary. However, over time we begin lowering our guard and return to our normal routines. Eventually, we focus on other priorities. Meanwhile, our adversaries patiently wait for the right moment to launch their next attack. It is our

collective challenge to understand and avoid this disastrous cycle and to maintain an appropriate level of alertness. Are you alert to what is happening around you, or are you caught in the daily grind and oblivious to the world? It is easy to slip into this vulnerable habit.

Immediately reporting AT-related problems, suspicious activities or incidents to your local security officials is the most critical responsibility you have. If you observe a lax security practice, a broken lock or inoperative security lighting, report it, report it, report it! Deterrence begins with maintaining a strong security posture, and if any member of the team is slipping, help all of us out and notify the appropriate office so it can be fixed. Every person affiliated with the agency is another set of eyes and ears to monitor for trouble.

Never assume that something has already been reported. If you see something, report it! Do you know the telephone number and e-mail addresses to report AT-related problems, suspicious activities or incidents? Suspicious or unusual activity should be immediately reported to your local security force — in most cases it is the DIA Police protecting the facility. When traveling outside of DIA facilities, suspicious or unusual activity should be reported to local law enforcement. Other information not of an immediate or emergency nature should be reported to your local FATO or your special security contact officer.

The next time you hear someone talking about antiterrorism, it will not be an abstract concept. You will know what it means in real terms and your role in it. If you have AT-related questions or suggestions, contact your local FATO, or the DIA AT Team by telephoning (703) 907-1899 or e-mailing Antiterrorism/Force Protection Service on JWICS.

Unofficial Foreign Contact REPORTING

By Victor R. Bryant and Dr. Daneta G. Billau, DA

Reporting unofficial foreign contact helps security officials isolate potential risks to our personnel and classified information around the world. Read on to find out everything you need to know.

Employees who joined DIA in recent years may still be adjusting to the way DIA does business, or if you're a seasoned veteran, you may need a refresher on the agency's foreign contact procedures. This article tells you everything you need to know when it comes to reporting unofficial foreign contacts. Reporting these contacts helps security officials isolate potential risks to our personnel and classified information around the world.

Reasons to Report

There are several compelling reasons to report unofficial foreign contacts. For starters, following regulations will help you avoid the appearance of impropriety. You also have the personal benefit of avoiding situations that may escalate to an untenable outcome. In addition, when you report you provide information that may be very helpful to the agency. Your reporting could assist security officials to identify foreign nationals who contact multiple employees and would otherwise go unnoticed, or you may help identify separate foreign contacts with similar characteristics. The Directorate for Mission Services' Counterintelligence and Security Office (DA/DAC) needs to know about all contacts with foreign nationals that involve unusual or suspicious circumstances.

Your Role

Now you understand your responsibility as a DIA employee to be aware of reporting requirements about unofficial contacts with foreign nationals and to report them. If you're a manager, you also need to know about unofficial foreign contact reporting so you can facilitate the reporting and communication between your employees and DAC personnel. By submitting unofficial foreign contact reports, you will help the agency secure personnel and information, and you'll avoid ramifications for failure to report or under report. So, let's get started.

The Directorate for Mission Services' Counterintelligence and Security Office (DA/DAC) needs to know about all contacts with foreign nationals that involve unusual or suspicious circumstances.

What to Report

You are getting the feel now of what to report, so to help you, here is a short list of unofficial foreign contacts you definitely need to report:

- Immediately report any contact with a foreign national (non-U.S. citizen) that leads you to believe there is a terrorism, espionage, sabotage or subversionary attack planned or occurring against U.S. citizens or interests.
- Within three days of contact you will need to report:
    - Any contact with a foreign national that seems unusual or suspicious; involves a business or financial relationship; or seems like an attempt to exploit you, the employee.
    - Any contact with a known or suspected employee of a foreign intelligence service, foreign diplomatic corps or international organization.
- If you have a second and continuing contact with a foreign national, you must report it within seven days.

- Report within 14 days, any initiation of "close contact" with a foreign national (defined as establishing bonds of affection or obligation, continuing intimate relations, cohabitation, or the intent to marry).

How to Report

Ready, set, let's start reporting! You need to fill out a DIA Form 12A and then submit it to the DAC Investigations Division. This is easy with the automated version on JWICS at http://www.dia.ic.gov/homepage/da_restored/da/daccsa/foreigncontact.htm or on SIPRNet at http://dh.dia.smil.mil/DAOSupport/WebForms/Contact.htm (be sure to use your SIPRNet e-mail address here). Or, you can request an electronic copy on NIPRNet by e-mailing victor.bryant@dia.mil. If you prefer, you can fax your DIA Form 12A to (703) 907-1709.

How Often to Report

A good rule of thumb for how often to report unofficial foreign contact is to report each instance of a foreign contact asking you about your work at DIA. In other situations, once you have reported your initial contact with an individual, then you only need to additionally report the original contact again when something unusual or suspicious happens or the type or frequency of contact significantly changes, such as from a business associate to paramour or cohabitant to fiance. You also need to make sure to separately report subsequent contacts introduced to you by the initial foreign national, i.e., relatives, friends, etc.

Special Situations

DAC knows there are always special situations that give rise to questions. You can get additional information about foreign contact reporting, special situations involving "close contact" and detailed information about foreign contact reporting responsibilities by looking over DIA regulation (DIAR) 50-17, which can be found under issuances on the Office of the Chief of Staff website. For more information, please contact special agent Vic Bryant, program manager in DAC's Investigations Division, at (703) 907-1801, or (VOIP) 982-5088.

CAPTURING Hearts and Minds

By Adrian "Zeke" Wolfberg, CS

Summary: Making someone change when they don't want to can be difficult, but not if you take small steps to create a big change.

This issue's book review is on "Switch: How to Change Things when Change is Hard" by brothers Chip and Dan Heath. The authors wrote "Switch" because their research in psychology and sociology showed that a successful individual, organizational or societal change follows a pattern involving our emotions, our intellect and our context. In situations where people embrace change, like getting married, having children or grandchildren, or getting a new job or home, we initiate our own change of behavior to accommodate the new conditions in our environment. We embrace the change. The Heaths' book addresses situations where change is not embraced.

In the early 1990s, Robyn Waters had her dream job: a high-end fashion job at an upscale department store, frequently traveling to Italy and attending meetings with Armani and Versace. Then she got laid off, a change she did not want. She found herself working at Target as the "ready-to-wear" manager responsible for sweats and t-shirts. The mindset at Target had been to "copycat," figure out what sells this year, have the product made cheaply, and sell it next year for half the price. The CEO wanted to change this longstanding mindset by riding the trends instead of lagging behind them. While Waters embraced the change in philosophy, most managers did not know how to change, and she had no mandate or power to advance this trend-right vision. So she started small.

For a time, trendy clothing was neutral in color. One season, color exploded onto the fashion scene, but Target remained numbers-driven. Managers saw that color did not sell the previous year, hence buyers were not motivated to buy color. So Waters went to a candy store and bought bags of brightly colored M&Ms and displayed them in glass bowls at her internal meetings, prompting a very positive reaction. She convinced one Target computer buyer to bring in the new (at the time) Apple iMac

SWITCH
HOW TO CHANGE THINGS WHEN CHANGE IS HARD
CHIP HEATH & DAN HEATH
THE BESTSELLING AUTHORS OF MADE TO STICK

Title: Switch: How to Change Things when Change is Hard

Authors: Chip Heath and Dan Heath

Published in 2010 by Broadway Books

Chip Heath is a professor at the Graduate School of Business at Stanford University

Dan Heath is a senior fellow at Duke University's Center for the Advancement of Social Entrepreneurship

computers in lime, strawberry, grape and tangerine colors, and that caused an even bigger positive reaction and increased sales. Color gradually became a decision factor by Target consumers, riding the fashion trend instead of lagging it.

How did Waters help to change Target? Waters knew that purchasing decisions needed to shift from last year's bottom line to what was fashionable today. She realized that if you want people to change, the change effort has to attract the person's emotional attention and has to link into the decision cycle of the organization. She used the colored M&Ms to trigger the emotional "aha!" When we try to change people's behavior, we are tinkering with their comfort zone and with behaviors that have become automatic and habitual. Stimulating an emotional reaction often unfreezes those habits.

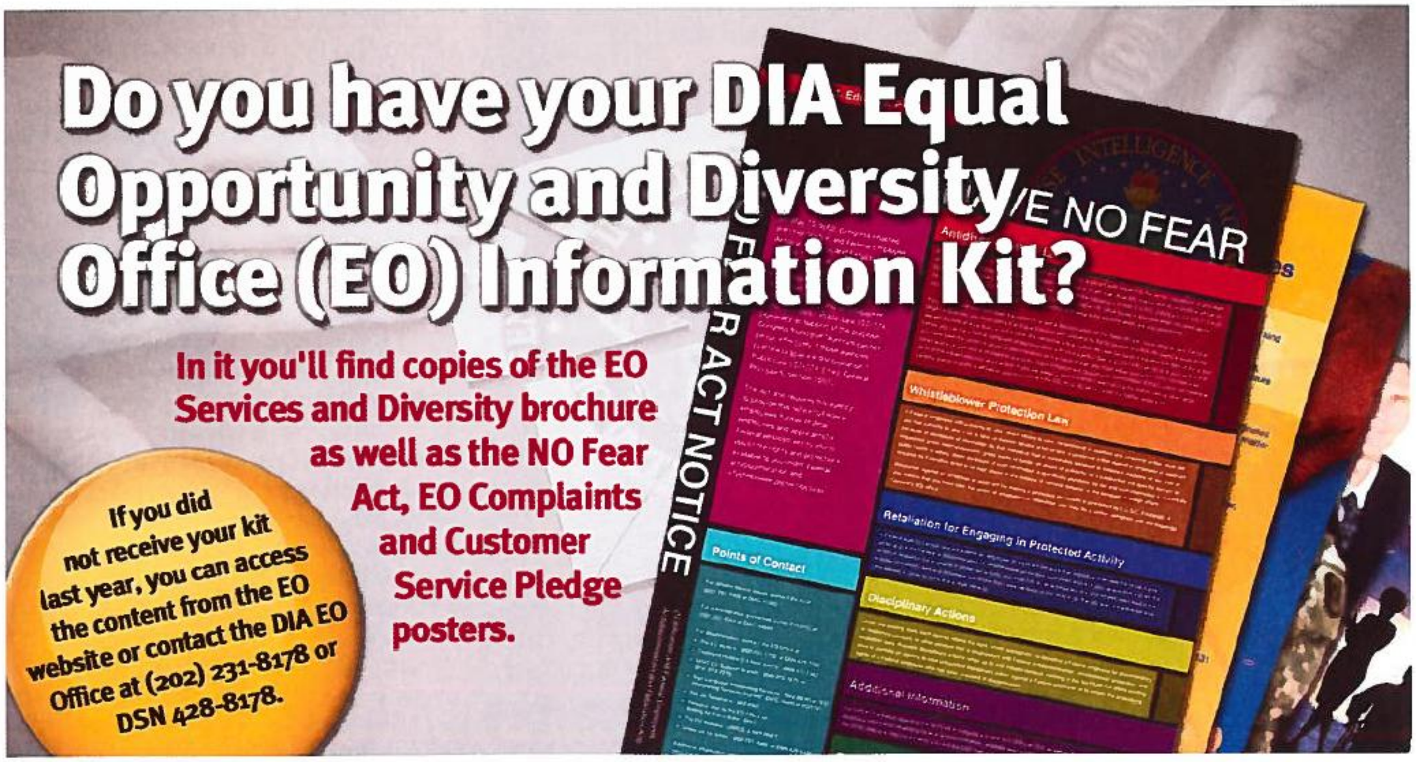
Waters realized that once she focused people's attention on color, she would have to take small steps to integrate something new into existing purchasing decision cycles. If we want people to change, we have to provide clear and concrete direction. Waters sequenced her color changing efforts to show incremental success, first with turtlenecks, then iMac computers, and then polo shirts. Without clarity of purpose, in this case the shift away from cost to fashion as the main driver, we can interpret the desired change in many ways, and perhaps none in the direction of the desired change. In Waters' case, unless the purchasing managers understand how a focus on fashion actually benefits an improved bottom line, the purchasing managers will not be inclined to change their purchasing behaviors.

Waters had no resources or authority to do what she did. She realized that to change someone's behavior, you have to change the mindset and environment in which they operate. To demonstrate success, Waters had to borrow people from other departments; sharing employees among departments had not been a Target management practice. Gradually, managers were willing to lend people because of the tangible benefits to their department.

What Waters did was effectively navigate Target managers' emotional and rational sides, which presented both opportunities and risks. She tapped into emotions to create energy and drive, and into the rational decision-making side to provide direction and long-term planning. Waters successfully avoided the risks of engaging emotions and making short term losses, as well as connecting the rational side and falling prey to overthinking and bureaucracies. Figuring out how and when to use an opportunity or turn a risk into an advantage is part of shaping the path for change to take hold.

Finally, the Heath brothers provide numerous findings from research. To begin a change effort, focus on the positives, and begin with what is working and how it can be improved, rather than fixing what is wrong. Big problems are rarely solved by big solutions; small goals lead to small victories. Small victories can often trigger a positive trend in behavior. People do not see how organizational and social context shapes individual behavior, instead attributing fault to individual personalities.

The Knowledge Lab purchased 30 copies of "Switch" for DIA civilian or military employees for their professional development. If you are interested in borrowing a copy, please contact Zeke Wolfberg at (202) 231-6449.



Do you have your DIA Equal Opportunity and Diversity Office (EO) Information Kit?

In it you'll find copies of the EO Services and Diversity brochure as well as the NO Fear Act, EO Complaints and Customer Service Pledge posters.

If you did not receive your kit last year, you can access the content from the EO website or contact the DIA EO Office at (202) 231-8178 or DSN 428-8178.

PROTECTING Critical Defense Infrastructure One Partnership at a Time

By Kristopher C. McQueen, DDC

Don't let the acronym confuse you. This DCIP — the Defense Critical Infrastructure Program — is bringing organizations together to protect critical defense infrastructure and keep us safe.

One of the most significant historical gaps in the Defense Critical Infrastructure Program (DCIP) community is the lack of specific and timely threat information to assess risks to critical infrastructure. As a risk management program, DCIP is not effective in understanding risk unless all organizations have access to pertinent threat and hazard information. In many cases, threats to critical infrastructure may not be apparent in the course of routine intelligence analysis. In fact, the intelligence community (IC) may not be actively identifying, disseminating and coordinating intelligence throughout the Department of Defense (DOD) on a threat capability or intent to specific infrastructures because the community may be unaware of nominated critical DOD assets and systems. Harnessing the full capabilities of the IC will enhance the accuracy of DCIP risk assessments.

Recognizing the need to improve intelligence support, DIA's Office for Homeland Defense and Defense Critical Infrastructure Protection has undertaken a multipronged effort in support of DCIP. This includes strategic national assessments, coordination of regional threat and hazard assessments, and ad hoc intelligence production for analysis of threats to critical infrastructure. Each of these efforts directly complements the DOD manual on Enhanced Threat and Hazard Assessments (ETHA).

The first step in this process is the formal tasking for support and coordination with all IC members, including service and combatant command intelligence components and national-level intelligence agencies. As the lead agent for the DOD intelligence sector, DIA's Office for Homeland Defense and Defense Critical Infrastructure Protection drafted an instruction covering the IC's support to defense critical infrastructure. This intelligence support policy will be issued by the undersecretary of defense for intelligence (USD(I)). The basic foundation of this intelligence support is the development of a triennial strategic global assessment of threats to critical infrastructure. The first such assessment was completed in 2009. Additionally, the instruction will require geographic combatant command intelligence components to provide the DCIP community with theater-level, area of responsibility-specific threat assessments. These regional assessments will assist asset owners in conducting their site specific assessments under the ETHA guidelines.

> "Harnessing the full capabilities of the IC will enhance the accuracy of DCIP risk assessments."

Finally, the intelligence support policy establishes an Intelligence Support to DCIP Working Group chaired by the chief infrastructure assurance officer (CIAO) for the intelligence sector. The CIAO is a senior-level leader from DIA who administers the intelligence sector and oversees all DOD intelligence community support to the DCIP. This working group will address the particular intelligence needs of the DCIP community and ensure adequate support. When necessary, the working group will cooperate with national agencies to request additional specific intelligence collection and production in support of the DCIP community's needs.

The intelligence sector has already increased intelligence support to DCIP through several projects in response to urgent overseas critical asset analysis. A pilot project to assess vulnerabilities at overseas facilities through the use of intelligence analysis proved the viability of this capability. The success of this pilot project will deepen collaboration between the IC and DCIP community. The intelligence sector is continuing to work with DOD's Defense Critical Infrastructure Office to enhance this relationship and initiate the intelligence support to the DCIP working group. This effort will ultimately involve all members of the DCIP community and will provide support to all DOD components in assuring critical assets. ◆

Command Training Facility 'PUNCHES ABOVE Its Weight'

By Peter G. Park, EUCOM

Molesworth's Regional Joint Intelligence Training Facility works with the State Department to teach intelligence and analysis to military and civilian personnel from African and European countries.

"When you're training your own forces, you take a lot for granted as far as shared systems and concepts go. When you're training partner nation forces, you can't take any of that for granted because the way they've learned is so completely different," noted Tracy Colley, lead instructor for the recent Military Intelligence Basic Officer Course — Africa (MIBOC-A) taught by the Molesworth, United Kingdom-based Regional Joint Intelligence Training Facility (RJITF).

RJITF supports both U.S. European Command (EUCOM) and U.S. Africa Command (AFRICOM) in training U.S. personnel and in presenting courses in both European and African countries in support of strategic engagement that infuses core capabilities, enabling interoperability both with the U.S. and among the nations themselves. With less than 35 instructors and support staff, the RJITF taught 499 courses in 2009 to 5,375 students, including 329 military and civilian personnel from 38 African and European countries as part of EUCOM and AFRICOM partner nation engagement initiatives.

The MIBOC-A program fosters the Trans-Sahara Counterterrorism Partnership Program, a U.S. State Department-led initiative developed to build regional capacity, promote interoperability and strengthen inter-regional cooperation in the trans-Sahara region. Supported by U.S. Marine Corps Forces Africa, MIBOC-A provides training on the basic intelligence cycle, analytic processes and tools, intelligence planning and collections, functional staff integration, and how to share information in a multinational environment.

In the December 2009 iteration of MIBOC-A, 23 officers from nine African nations, along with one U.S. officer, graduated from a 12-week introductory intelligence course at the Gendarmerie Academy in Dakar, Senegal. The course equipped junior officers with skills to operate in a battalion-level military intelligence staff.

"We are building our Army after 14 years of civil war," said a Liberian officer. "I am the first infantry officer sent abroad for this training. I came [here] with little training, but high expectations, and I am very, very pleased with it."

"The African officers are highly motivated to learn," said Colley. "It's impressive. If they're into a practical exercise, they won't go to lunch. We have to literally force them to leave their table and go to lunch. Our partner nations send their best officers, and it's obvious by the way they carry themselves."

Networking among fellow African officers is an important goal of the course. "I met a lot of good friends here," a Mauritanian student said. "I know we're going to keep in touch as we move forward in our careers."

Photo courtesy of RJITF

Students from Burkina Faso, Cape Verde, Liberia, Mali, Mauritania, Nigeria, Tunisia and the United States put the finishing touches on a briefing during the recent Military Intelligence Basic Officers Course — Africa training held in Dakar, Senegal. This 12-week course, taught by a team of instructors from RJITF, prepares young African officers for duties as unit-level intelligence officers and to operate in a multinational environment.

Terrance Ford, director of AFRICOM's Intelligence and Knowledge Directorate, spoke to the students during their graduation ceremony.

"While the United States and Senegal provided much of the support and facilities for MIBOC-A, the U.S., like all militaries, learns a great deal from

partner nations when we sit and listen to your ideas, your experiences and your concerns," said Ford to the students.

RJITF instructors were joined by guest instructors from Senegal, Burkina Faso and Mali, indicative of plans to eventually have a course primarily taught by former students from African nations.

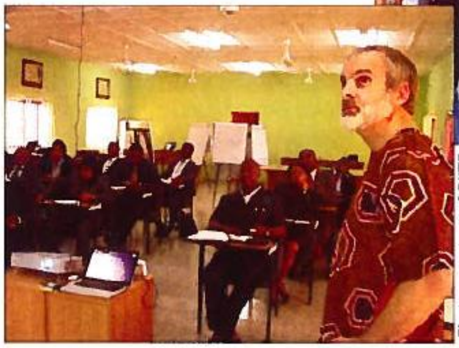
"We would still like a role in it, because we're part of the partnership," said Colley. "However, the goal is for them to become the trainers as time goes on."

MIBOC-A is just one of several partner nation courses taught by RJITF. In February RJITF instructors Todd Sears and Cynthia Lenhart conducted a successful critical thinking and structured analysis (CTSA) workshop in Abuja for the Nigerian Defense Intelligence Agency (DIA). According to Sears, "When students were asked what they considered the high point of the course to be, the answers were cast as wide as a Nigerian evening vista."

"I had an awesome week; a total departure from other classroom experiences," said Omobolanle Sabiu of the Nigerian DIA. "The atmosphere was conducive to learning and the instructors were relaxed and friendly. They broke down the process into its barest essentials for better assimilation. I made friends, learned to collaborate on finding solutions to intelligence requirements, and enjoyed myself."

RJITF also supports a version of the basic course for European partner nations,

RJITF instructor Todd Sears makes a point to MIBOC-A students. The course conducted by the RAF Molesworth RJITF is a component of U.S. Africa Command's partner nation engagement. ▼



Photos courtesy of RJITF

TEACHING Iraqis to TEACH Iraqis

By Maj Rich "Checker" Greenslit, HC

The Directorate for Human Capital is bringing critical thinking and analysis to Iraqis.

On Sept. 10, 2009, I departed the United States to travel to Camp Taji, Iraq. My mission: Train Iraqi intelligence instructors to teach intelligence analysis. Though cobbled together from several courses, the course I brought them retained the core critical thinking and structured analysis (CTSA) elements: emphasis on critical thinking, inclusion of an analytic process, introduction of structured analytic techniques and a focus on achieving analytic standards.

The most important work began as soon as I arrived at Taji — translation. I had to make sure the slide and exercise translations were complete and consistent. For this, my translator, Nahrouz Hajo, was absolutely critical. Indeed, I realized during this trip that successfully teaching in a foreign language depends upon a strong instructor-translator partnership.

I began teaching Sept. 26. The class consisted of 19 students — 15 Iraqi military students pulled from division-level intelligence and four Iraqi instructors assigned to the school. I used standard CTSA instruction techniques, combining lecture with healthy doses of exercises and open-ended questioning. I also tried to engage the students using illustrative video clips and "Spy vs. Spy" cartoons. This all seemed to work, and after a few days we seemed to bond as a class. We enjoyed our time in class, and the students generally became engaged with the material.

Maj Rich "Checker" Greenslit presenting to the class in front of the "big board." On the sides of the board, the main terminology is captured in both English and Arabic, including concept, purpose and assumption.

Another important addition to the class was the "big board." I only had one usable whiteboard, but we found it useful to capture key course concepts around the margins in both English and Arabic. This served as a constant reference for both the students and Hajo, while allowing me to physically point to the concept I was focusing on.

Throughout the course students practiced various structured techniques, following Heuer's analytic process, using the same CTSA message traffic we normally use — the liquid natural gas tanker in New York harbor. I was apprehensive heading into the first problem restatement exercise, as I was not sure students would understand the material. Perhaps it was too U.S.-centric. Perhaps it was too far removed from anything they had

▲ RJITF instructor Robert Blair leads a seminar session during an intelligence workshop in Constanta, Romania. The group included civilian and military intelligence officers and analysts from the Romanian armed forces and Ministry of Defence.

MIBOC-E, which has been taught in Georgia, and various targeted intelligence seminars that run from CTSA, intelligence planning, intelligence support to targeting, and international combating terrorism.

In response to a request from the director of intelligence of the International Security Assistance Force (ISAF), RJITF is rolling out a new Expeditionary Intelligence Training Course to train NATO personnel deploying to serve in ISAF intelligence billets in Afghanistan. The hands-on training covers essential deployment tasks including ISAF systems and tools familiarization. Portions of the course were scheduled to be piloted with the ISAF Intelligence Orientation Course, led by the NATO School in Oberammergau, Germany, in April, and the full course was presented in Portugal at the end April.

"I'm proud of the RJITF staff and our role in providing high-quality, advanced intelligence training for our U.S. European Command and U.S. Africa Command analytic cadre and in building capacity and relationships with our partners across Europe and Africa," said RJTF Director Mike Redding.

"The RJITF excels in creating something from nothing and recently received a DNI award for their work," said Col Pete Devlin, JIOCEUR Analytic Center commander, about his RAF Molesworth-based unit.

As Devlin sums it up: "The RJITF punches way above its weight."

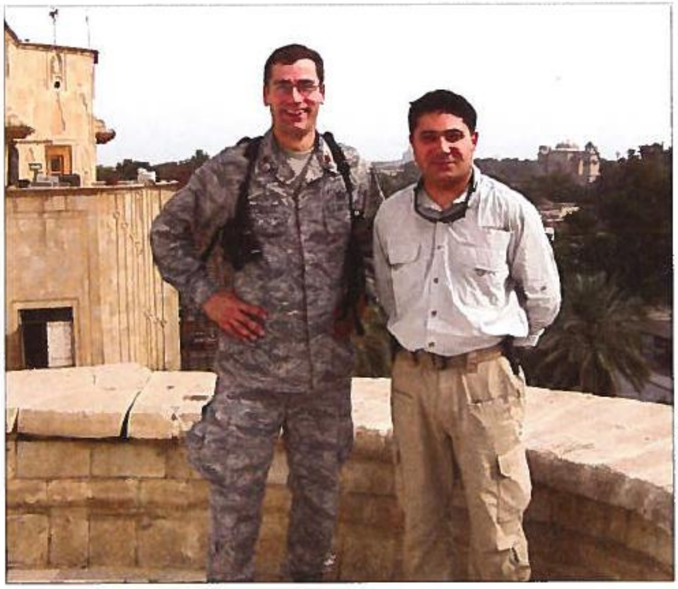
Note: Portions of this article are based on a piece by Sgt Lydia M. Davey, Marine Corps Forces Africa.

experienced before. Yet the students did exceptionally well, breaking down the problem and identifying the most critical questions involved.

For a final assessment of the class, I had groups of students present an intelligence brief, complete with bottom-line-up-front, alternative hypotheses and caveated assessments and evidence. I was pleased with the results; the groups presented briefs on par with what I would expect from beginning U.S. students.

The Iraqi instructors began teaching Iraqi students Nov. 14. Frankly, I was scared on that first day, unsure of how it would go. Yes, my class had gone well, but if the Iraqis could not teach the Iraqis, the whole trip was wasted. Contrary to my fears, however, the Iraqi instructors did extremely well. They had a firm grasp of the big-picture aspects of the course and were able to convey them clearly and repeatedly to the students. The instructors generally used the same examples I had, sometimes even copying my exact words, but did so without reading their notes or reciting from the slides. They established a positive classroom atmosphere and the final briefs from the student groups were acceptable. I was impressed.

All of this is not to say that the train-the-trainer trip was without problems. Both classes had a few students either unwilling or unable to learn the material. We had a typhoid outbreak. We lost a student when he was kidnapped by the Peshmerga from his hometown and another student went AWOL to recover his belongings from his brothers-in-law. One student lost a relative in the December Baghdad bombing. In the end, however, I felt that the effort was successful, and the Iraqis have an intelligence analysis course they can teach themselves.



Photos courtesy of HC

Maj Rich "Checker" Greenslit and translator Nahrouz "Big Joe" Hajo during a short trip to Baghdad.

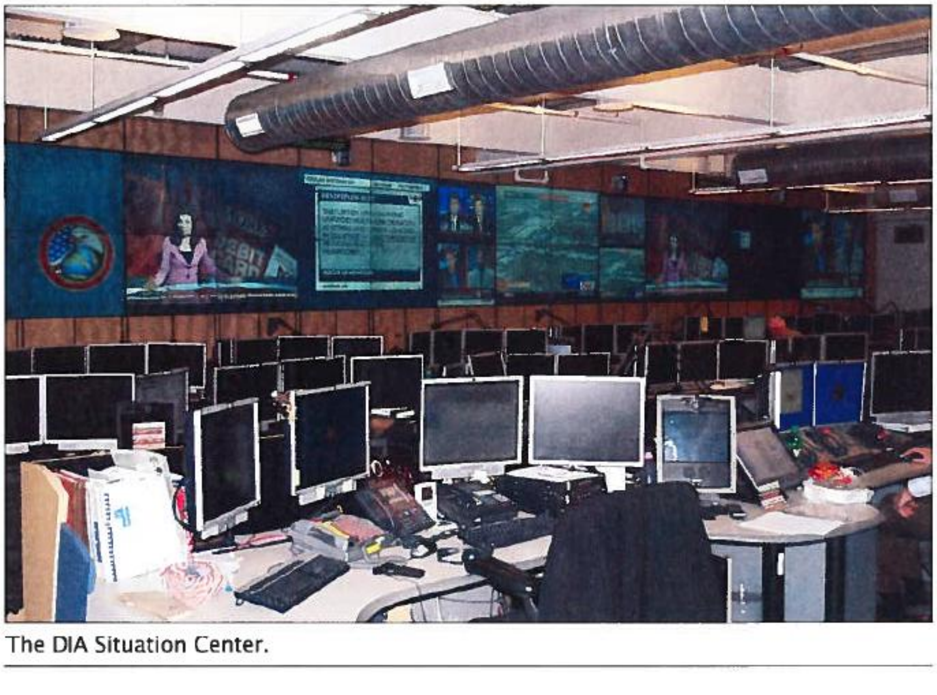
SITCEN Keeps Leaders IN THE KNOW

By Scott K. Muessig, DA

DIA's Situation Center is working around the clock to keep our leaders in the know on all things affecting the agency.

DIA operates a 24/7 situational awareness watch desk, known as the Situation Center, or SITCEN. Collocated with the Global Intelligence Operations Center, the SITCEN provides situational awareness to DIA senior leadership on matters pertaining to the agency's operational capability worldwide, the status of personnel and facilities, and things that may impact DIA's ability to support its global mission. Watch officers obtain data from various sources, validate the information as necessary and report daily to senior leadership. Personnel from the Directorate for Mission Services' Office of Enterprise Operations (DA/DAE) work in the SITCEN.

Collaboration is key with watch officers coordinating issues with other watches and offices such as the Directorate for Human Intelligence (DH) desk at the National Military Command Center, the Directorate for Information Technology and Chief Information Officer (DS) Watch, the Office for Engineering and Logistics (DAL) and the Law Enforcement Desk. Watch officers monitor news sources, other command/operations centers and additional sources for relevant information. In the event of an emergency during non-duty hours, the SITCEN acts as the DIA Emergency Operations Center until appropriate staff can respond.



The DIA Situation Center.

CONTACT INFO FOR THE SITCEN

Commercial
(202) 231-1900 or
1-866-HQ1-1DIA (1-866-471-1342)

TS VOIP
982-3524

JWICS
dise875@dodiis.ic.gov ("DIA Situation Center" in the Global)

SIPRNet
DIASituationCenter@dia.smil.mil

NIPRNet
DASCWatch@dia.mil

Watch officers are designated as emergency essential employees, continuously manning the SITCEN. They write daily situation reports and notifications on issues affecting DIA infrastructure, personnel or operations, and track succession of senior leaders. The SITCEN receives, drafts and transmits personal event notifications (PENs) on DIA personnel to support casualty affairs officers and other action officers in the agency.

The SITCEN's daily situation report is on JWICS at http://diateams.ne.dodiis.ic.gov/sites/DA/DIA_SC/default.aspx. The site also includes the SITCEN mission briefing, PEN template and archived situation reports. Employees are also reminded that family members can call the SITCEN for help on various issues. The SITCEN can assist family members who are unable to contact deployed DIA employees and help families obtain access to agency services.

Detachment of the Month

Force Protection Detachment SOFIA

By the Force Protection Detachment Staff, DX

Editor's note: The Communiqué will now be alternating the traditional Post of the Month feature and a new feature, Force Protection Detachment (FPD) of the Month. The FPD program is a Department of Defense (DOD) and Department of State initiative to expand and permanently place DOD special agents in overseas locations. DIA maintains oversight as the DOD program manager providing resources and manpower. In just seven years of existence, the program has expanded to more than 30 locations worldwide and is expected to continue to grow. The FPD program falls under the purview of the Defense Counterintelligence and HUMINT Center (DX).

For an introduction to the FPD program, see the May 10 issue of the InterComm.

Country Highlights

Force Protection Detachment (FPD) — Sofia is in the southeastern European country's capital city. Bulgaria, nestled along the western reaches of the Black Sea, is roughly the size of Tennessee and shares land borders with Serbia, Macedonia and Turkey, as well as two European Union member states, Romania and Greece. Bulgaria maintains security over 230 miles of Black Sea coastline, including the major tourist beaches of Primorsko in the south, Sunny Beach in the center and Golden Sands to the north. Two points of interest along this coastline are the port cities of Varna in the north and Burgas to the south, both of which thrive on regional and international commerce, as well as NATO-related naval activity.

ROMANIA
SERBIA
BULGARIA
Sofia
TURKEY
MACEDONIA
GREECE
Agean Sea

Bulgaria achieved its independence in 1908, following five centuries of Ottoman rule. Bulgaria entered World War II as an ally of Germany, but shifted its allegiances by war's end and aligned itself with the Soviets to fight its former ally.

Bulgaria remained communist until 1990, when the country held its first multiparty elections since the 1940s. Bulgaria's citizenry endured a severe economic crisis in the mid-1990s as the country struggled to shed the remnants of communism and now, almost two decades later, Bulgaria continues to face challenges. The struggle to strengthen its economy, reduce unemployment and combat corruption is undermined by a strong

▲ FPD Sofia members in the courtyard of the U.S. Embassy (from left to right): Investigative Assistant Zornitsa Dimitrova; Special Agent in Charge Michael Kenville; Special Agent Sean Alkins. In the background, Mount Vitosha looms in the distance and statues of the "First American Diplomats," stand behind the FPD members.

organized crime base. Still, Bulgaria continues its efforts to ensure its place within regional and global spheres of influence. Bulgaria joined NATO in 2004 and the European Union in 2007 in moves to assimilate with its new friends in the West.

Detachment Highlights

The Air Force Office of Special Investigations (AFOSI) is the executive agency for FPD-Sofia, currently supervised by AFOSI Special Agent in Charge Michael Kenville. Kenville arrived in January 2007 to establish the detachment, and his initial efforts focused on standing up the office and developing sound and effective force protection relationships with both host nation counterparts and the U.S. Embassy Country Team.

The FPD was fortunate to bring aboard Zornitsa Dimitrova as the investigative assistant and coordinator. Dimitrova is a local employee who boasts an extensive background in investigations, working with Bulgarian security/law enforcement personnel and four years of experience working with the Defense Threat Reduction Agency and the Department of Energy. Dimitrova supported her first U.S. Navy ship visit in early 2009, and continues to broaden her FPD experience. In 2008 the U.S. ambassador approved the arrival of U.S. Army Military Intelligence Special Agent Sean Alkins, raising the detachment's office manning level to three.

There is never a dull moment for an FPD agent, and the moments spent at work by the members of FPD-Sofia are no exception. Most DOD activities occur outside Sofia, requiring FPD members to spend the majority of their time on the road. The FPD supports training sites in Plovdiv, Yambol and Sliven, as well as U.S. Navy visits in Varna and Burgas. In addition to working with Bulgarian counterparts at these locations, FPD personnel routinely travel to conduct hotel, route and port assessments and to obtain up-to-date threat information. In 2008 FPD-Sofia supported 25 DOD exercises, operations and port visits involving more than 75 aircraft, 13 U.S. Navy and Coast Guard ships, and more than 5,600 DOD personnel, as well as 20 senior DOD visitors. Activities supported bilateral training, real-world operations, military-to-military visits and counternarcotics interdiction cooperation on the Black Sea.

In less than three years, FPD-Sofia stands as the country team's focal point for counterintelligence and force protection support to in-transit DOD activity in Bulgaria. With nearly 1,000 separate DOD activities in 2009 and no U.S. base to support military-to-military engagements, the FPD is poised to play a key role in maintaining the country team's situational awareness on the region's potential threat environment. The FPD team members are the "tip of the spear" for countering potential threats against DOD personnel and property in Bulgaria.

In June 2009 FPD agents supported the arrival of the U.S. Coast Guard Cutter Dallas and crew at Burgas East Port Facility, Burgas, Bulgaria. ▶

U.S. COAST GUARD
716

◀ In September 2009 FPD agents supported the arrival of USS Taylor to Varnas East Port Facility, Varnas, Bulgaria.

2010 IC Collection Assessments Conference

By Jacob Ulvila, NIC-C, and John R. Jones, DJ

You can play a part in guiding the future of collection assessments. Register by June 30 to attend the 2010 Intelligence Community Collection Assessments Conference.

The Defense Intelligence Operations Coordination Center (DIOCC) and the National Intelligence Coordination Center (NIC-C) are co-hosting the second annual Intelligence Community (IC) Collection Assessments Conference July 19 — 23 at the MITRE Corporation in McLean, Va. The conference is free of charge and is open to collection assessments practitioners from across the defense and intelligence communities. Register on JWICS at http://diocc.dodiis.ic.gov/portal/page/portal/DIOCC/ASSESSMENT COMMUNITY by selecting "2010 Conference" and then "Register."

This year's conference is co-hosted by Maj Gen Blair Hansen, DIOCC deputy director, and Gregory Moulton, director of the NIC-C.

Last year's conference resulted in a sharing of collection assessments best practices and the establishment of a collection assessments community of interest (COI) across the Department of Defense (DOD) and the IC. The 2010 conference will build on last year's results to identify the major areas of common concern to DOD and the IC and to develop a consensus roadmap to guide the future of collection assessments. This collection assessments roadmap will improve communications across DOD and the IC, focus scarce manpower and financial resources on action-oriented objectives, and promote the integration of collection assessments activities.

> "The 2010 conference will build on last year's results to identify the major areas of common concern to DOD and the IC and to develop a consensus roadmap to guide the future of collection assessments."

A highlight of the 2010 conference will be the executive discussion panel on July 22. Senior leadership will share their thoughts and insights on the proper role of collection assessments in DOD and the IC, their organizations' relationships with other assessment organizations, and the most important first steps toward integrated collection assessments policies, doctrine, procedures and standards. The panel will also answer questions posed by the audience.

All conference attendees will have the opportunity to participate in a series of working groups on the topics of collection assessments policies, the Defense Intelligence Cycle Assessment Methodology (DICAM), collection assessments measures of effectiveness and performance, and professionalizing the collection assessments work force. Working groups will consider requirements, policies, procedures, standards and implementation. Recommendations of the working groups will be briefed to DOD and IC leadership on the final day of the conference and will form the basis for the collection assessments roadmap.

To register or for any questions, contact John Jones, DIOCC Assessments Division, at (202) 231-1150, secure 982-1801 or john.jones@dodiis.ic.gov, or see the conference JWICS website http://diocc.dodiis.ic.gov/portal/page/portal/DIOCC/ASSESSMENT COMMUNITY.

2010 IC Collection Assessments Conference

Interview with Bill Mills

Director of the National Media EXPLOITATION CENTER

By the Communiqué Staff, CP

The Communiqué staff met with Bill Mills, director of the National Media Exploitation Center (NMEC), to talk about his first few months as director of a national intelligence center, the strategy for NMEC in Afghanistan, current challenges the organization is facing and NMEC's move under the Directorate for Technical Collection (DT).

Mills has served as the director of NMEC since December 2009. Prior to this appointment, he was the chief of the Defense Resources and Infrastructure Office (DRI) within the Directorate for Analysis (DI). He began his career at DIA 25 years ago as an analyst in DI, and has served in the Directorate for Human Intelligence and the Command Element, and on the Office of the Director of National Intelligence (ODNI) staff.

Photo by Jane A. McGehee, CP

Bill Mills, director of NMEC, sat down with Kate Worley from Internal Communications to discuss his new role as the director of a national intelligence center, emerging mission requirements and challenges facing the organization.

COMMUNIQUÉ: *You have been in your role as director of NMEC for just a short time. Has there been anything that has surprised you about the organization?*

MR. MILLS: I have been at NMEC about five months, and there is still a lot to learn about the operation. I knew the basics of document and media exploitation (DOMEX) before joining the center. I understood that data finds its way here, is processed and stored, then exploited, and finally reported out. What surprised me was the rigorous and complex process that is in place to do all that. The amount of data that NMEC receives and stores is incredible. I didn't know what a terabyte was until I got here, and the center deals with about 20 to 30 terabytes of data per month. There is a process in place to handle this vast amount of data and the noxious content that goes with it, such as bugs, worms, viruses and pornography. We sort through all that to find the information that is of intelligence value and report it out to our customers.

Another surprise was the sheer requirements workload that the center maintains. We have an operations meeting every week, and last week we were working 190 active requirements from 14 different customers.

COMMUNIQUÉ: *What perspectives did you bring coming from the analytical side of DIA?*

MR. MILLS: Previous to this job I didn't have an appreciation of the value of DOMEX. DOMEX is different from all of the other intelligence sources, and it tends to fall in the seam. It is specifically not open source or signals intelligence. It is media that the U.S. acquires, captures or owns. Before coming to NMEC, I didn't understand how unique this source of data is to analysts, so I am pressing my staff to reach out to a broader set of analysts and encourage them to become familiar with the value of DOMEX and the unique capabilities of NMEC. We are reaching out to analysts because at this time they can't access our data from their desktop. Analysts can work

NMEC STATS

Government civilian:	**58**
Embedded LNOs:	**63**
Contractors CONUS:	**294**
Contractors OCONUS:	**250**
Total footprint:	**665**

HISTORY

After Sept. 11, NMEC was chartered by the director of central intelligence to become the nation's foremost proponent and focus for the exploitation and sharing of the massive troves of captured and seized document and electronic media associated with the global war on terror.

with the data, but they have to be in the building due to the current information technology (IT) architecture and constraints from the noxious content. We have a plan to improve storage and access via our future DOMEX architecture called the National Exploitation System, or NEXSYS, which I'll expand on later.

NMEC is bringing in groups of DI analysts to educate them on the value of DOMEX. For example, NMEC hosted leadership from the Iraq Intelligence Cell a couple weeks ago. We also hosted two different sets of DI analysts working threat finance issues. We are reaching out to the Department of Treasury, too, because we think their analysts should become more familiar with the data we have from counterthreat finance operations in Afghanistan.

COMMUNIQUÉ: *Can you tell us a little bit about what it means to be a director of a national intelligence center?*

MR. MILLS: It is an honor to take over as director of NMEC. I was pleased that LTG Burgess had the confidence in me to take on this job. Roy Apseloff, who I replaced after his six years as the director, did a fantastic job, and he and his team basically built this place from about 30 people to a work force of hundreds of people. NMEC is making an impact every day and has developed into the pre-eminent DOMEX center.

Being a director of a national intelligence center means dealing with a different set of customers than I am accustomed to from my previous positions. The intelligence partnerships here are much broader than the set I worked with in DI, where my customer set was primarily from defense. NMEC has the same expectations of quality support to the combatant commands, the Joint Staff and the Office of the Secretary of Defense, but we are also serving the needs of law enforcement, homeland security and counterintelligence (CI) customers. The same can be said for collaborating with a larger set of stakeholders. NMEC has stakeholders in defense, but also in homeland security, law enforcement and at the Central Intelligence Agency.

Being an ODNI center also means you have to commit to collaborating, integrating and data sharing. If you are an ODNI center you have to walk that walk every day. I think NMEC does a very good job of that, but of course we can always do better.

COMMUNIQUÉ: *What is the strategic direction of NMEC with the draw down in Iraq and the build up in Afghanistan?*

MR. MILLS: Some of the customers we support in Iraq and Afghanistan will shift focus on other regions of the world. Some of that is happening now. NMEC's job is to figure out how to tie into those customers in various parts of the world. But regarding Iraq, NMEC will maintain a DOMEX capability there for the foreseeable future.

Making Media Exploitation MORE EFFICIENT

By Terry S. McCall, NM

Transmitting data from the field to NMEC's headquarters is getting faster and easier with the Tactical Storage and Area Network.

In order to meet its mission, the National Media Exploitation Center (NMEC) must ingest, send and receive large volumes of media from remote locations worldwide. The core component in transmitting this data remotely back to NMEC headquarters from forward locations is the Tactical Storage Area Network (TACSAN) system. The TACSAN system was initially developed to provide a "store and forward" capability at Joint Document Exploitation Center — Iraq (JDEC-I) at Camp Slayer, Baghdad. This initial development phase was termed TACSAN Phase I.

TACSAN Phase I provided the capability to rapidly ingest, or store, high volumes of forensically captured media and transmit it across dedicated communication lines from JDEC-I to NMEC headquarters for further media exploitation (MEDEX) and data archiving. TACSAN Phase I implementation included package (media) transmission verification, process status, system monitoring and basic reporting elements.

TACSAN Phase I was installed at JDEC-I in February 2009 and was deemed at full operational capability in April 2009. The TACSAN is attached to a 40 megabyte (MB) communications pipe that supplies the vehicle for data transmission. Since installation and initial operating capability, the TACSAN has transmitted approximately 13 terabytes of media to NMEC headquarters.

NMEC is currently developing the second iteration of its TACSAN platform, TACSAN Phase II. The NMEC Office of Information Technology gathered requirements from other internal NMEC offices, to include Operations, Collections Management and Forensics, for inclusion into TACSAN Phase II. These new requirements include the integration of state-of-the-art MEDEX tools for standardization of the MEDEX process, ingestion and transmission of encapsulated cell phone telephone exploitation data, and increased monitoring and reporting capabilities. TACSAN Phase II is tentatively scheduled for deployment to Afghanistan in the May/June 2010 timeframe, using a 16MB communications link between the JDEC-Afghanistan (JDEC-A) and NMEC headquarters. ▲

In Afghanistan we are increasing resources at our Joint Document Exploitation Center (JDEC) in Bagram and at its detachments, and we will also increase capacity back at NMEC headquarters to support the JDEC and customers forward. Although communications and bandwidth have been a challenge, NMEC near-term solutions are underway, and we expect to see an improvement by the end of the summer.

I also think that we are just starting to scratch the surface regarding NMEC's support to law enforcement and homeland security. Most of the data we currently receive is from Iraq and Afghanistan, but at the same time the data we exploit from law enforcement and homeland security has increased significantly. We maintain excellent partnerships with both the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). The future is bright, and although there is a heavy focus on wartime support, an increase in law enforcement, homeland security and CI operations is already happening.

We are trying to get the word out at all levels about NMEC's capabilities. It is important to educate law enforcement and homeland security elements so they understand that there is a national-level capability here to help them. Our forensic and linguist capabilities are tremendous, and it's a capability that can work for them.

COMMUNIQUÉ:
What are a few areas where NMEC is being challenged in an expanding Afghanistan mission?

MR. MILLS: I touched on the two big things earlier. One is increasing our footprint in Afghanistan, and the other is improving our communications. As most know, the U.S. military is surging in Afghanistan, and in the long run that will mean more work for NMEC. We are working hard to increase our capability there quickly.

Photo courtesy of NM

Iraqis practice cellular phone exploitation.

The other challenge is communication and bandwidth. NMEC continually seeks innovative ways to meet — or stay ahead of — the increasing requirements of our customers to ensure we provide them the time-sensitive intelligence they need. Within the current operating environment, we have identified the need for faster, more reliable methods of communication and have begun implementing solutions to address existing challenges.

NMEC: Technical Exploitation of Digital Media

By Tammy Poor, NM

Recover a cell phone in the middle of a war zone and need the intelligence from it? The National Media Exploitation Center's Forensic Office has the tools to do just that.

The clock is ticking. The door caves in and papers are swirling around a dust laden hideout in a small provincial town in Afghanistan. After securing the location, American soldiers collect papers, disks, phones, computers and other secure digital storage devices. The materials potentially hold plans, networks and strategies of the enemy. The plans may have current insurgent schedules, what target is next, and codes for detonating explosives. The networks may contain names, phone numbers, passwords and e-mail addresses of enemy personnel. The present value of this captured enemy material is decreasing every second it is not exploited and fused into intelligence for our warfighters and decision-makers.

The National Media Exploitation Center — Forensic Office (NMEC-FO) provides advanced technical exploitation services to intelligence, defense, homeland security, law enforcement and other United States government consumers. NMEC-FO provides targeted forensic examinations and digital media analysis as well as global operational support to media exploitation units in various countries. NMEC-FO provides a wide-range of specialized tools and capabilities in support of media exploitation (MEDEX), audio and video exploitation (VIDEX) and cell phone exploitation (CELLEX).

An ever-increasing number of personal computers are being used to commit or plan crimes. Digital investigations, or MEDEX, identify digital evidence and collect intelligence about the actions or intent of authorized and unauthorized computer users. A typical examination includes a bit-for-bit imaging of the media (hard drive, thumb drive, etc.), copying the image to another storage location (gold copy), and utilizing advanced digital analysis tools to analyze the contents.

Video provides a rich medium for rapid information sharing across international boundaries. Advances in

COMMUNIQUÉ: *What are a few things that our readers may not know about NMEC?*

MR. MILLS: Because of the noxious content within the media we receive, the NMEC TS//SCI exploitation work environment is closed. We receive media, whether a hard drive, thumb drive or video, and move that data into our closed environment because of the content. This limits access, which is why we have many partners and stakeholders located here in NMEC headquarters. We also have data storage challenges. What now amounts to terabytes of stored data continues to grow exponentially and has the potential to become petabytes of data in less than 10 years. The solution to manage this data is the National Exploitation System (NEXSYS). NEXSYS will feature a scalable, multitiered storage architecture as well as rapid parallel processing and exploitation capabilities.

We have established a program office for NEXSYS and we have an outreach program where we are bringing in stakeholders to work through the details. We see this as a positive because right now there are a lot of DOMEX stakeholders trying to solve the same problems and store the same data. With NEXSYS, NMEC will provide data storage and basic services, and our partners and stakeholders can access the data and apply new applications. There are savings across the board if we fully implement this; it will create a lot of efficiencies while centralizing data and capabilities. *[For more on NEXSYS, see page 24.]*

COMMUNIQUÉ: *Based on decisions made at the director's off-site meeting earlier this year, NMEC moved under the Directorate for Technical Collection (DT) at the end of March. What does this transition mean for NMEC?*

MR. MILLS: Art Zuehlke, the director of DT, envisions NMEC as a DT element that will remain an intelligence community (IC) center with the same mission and customers. But it will merge the center with a larger organization that has some of the same missions and challenges. When I first heard we were going to fold up under a DIA directorate, I thought DT made the most sense as both organizations have exploitation responsibilities. We have a lot of the same customers, such as law enforcement, homeland security and forward military customers. We share forward presence in theater, and there is ample opportunity for collaboration in Afghanistan.

DT and NMEC both have a sizeable contractor work force so there may be some streamlining there. Also, there may be efficiencies regarding research and development (R&D) initiatives. DT has an R&D effort, and NMEC invests in R&D to stay ahead of technology and as a means to look for more efficient ways of doing business. Lastly, both NMEC and DT are thinking in similar terms in regard to future global support.

Tara Johnson loads hard drives into the NMEC exploitation system.

Photo courtesy of NM

cheap, widely available video production hardware and software have created large volumes of video and audio data from a wide-range of sources that must be assessed by intelligence community (IC) analysts. VIDEX attempts to extract valuable content from these sources. NMEC provides an array of services to include analog to digital conversion, still extraction and enhancement, compression/decompression conversion, audio filtering and clarification, and metadata mining reviews of acquired media. Audio processing includes retrieving audio tracks from videos or cell phones in addition to extracting additional tracks for narration or translation.

Mobile device forensics, or CELLEX, is the science of recovering digital evidence from cellular phones, GPS and other personal electronic devices under forensically sound conditions and using accepted acquisition methods. The cell phone places a cheap and completely mobile communications and multimedia platform into the hands of entire populations. The tremendous growth in cell phones and electronic device usage worldwide represents both a challenge and an opportunity to the IC. The NMEC-FO CELLEX team offers a full range of technical exploitation services targeted to mobile devices to include data acquisition, examination and reporting.

The digital forensics community faces a constant challenge to stay abreast of the latest technologies. Enabling unprecedented levels of collection and exploitation opportunities, technical exploitation provides the IC unique insight into our adversaries' associations, intentions and capabilities. To meet the challenge of an ever-evolving future and to ensure our government's continued information dominance on the battlefield, NMEC-FO conducts research and development on emerging technology platforms to discern next generation exploitation tradecraft and methodologies. Additionally, NMEC-FO in partnership with the IC is working to develop common standards and practices for training, exploitation and reporting associated with technical exploitation.

NMEC-FO personnel provide a decisive advantage to our warfighters and policymakers by providing critical intelligence that is often not available by other channels. ▲

COMMUNIQUÉ: *What other management or organizational enhancements do you plan to implement?*

MR. MILLS: The organization is shifting toward becoming a 24/7 operation. NMEC received supplemental funding to increase capacity in that direction. The justification was to better posture the organization to exploit the volume of data we receive. NMEC's mission set is only going to grow as we ramp up in Afghanistan and more U.S. forces report there. Also, once the Army tactical DOMEX personnel are fully staffed in theater, that too will increase NMEC's workload.

Also, NMEC needs linguists, forensic examiners, media managers, IT specialists and platform managers working beyond 9 to 5. The platform managers handle theater customer requirements, the media managers ingest the media, the IT specialists store it and provide access, the linguists and forensic examiners exploit it, and the reports writers provide the product. We are not setting up a watch center, but rather extending our basic mission into off- hours to meet our customer needs.

Another thing that I'm focusing on is joint duty assignments. NMEC has done that in the past with limited success, so we are going to give that a hard look. We would like to get the assignments posted in the next few months. NMEC has positions that require a variety of skill sets, including operations, IT, forensics and policy, so it's a great opportunity to bring in some talent from the outside while providing joint duty credit.

Also, the leadership team has started developing an implementation plan to identify NMEC responsibilities and investment areas. IC Directive 302 defines DOMEX, what NMEC does, who it reports to and its relationship to the ODNI. ICD 302 also tells me that as director of NMEC, I need to be doing or accomplishing a lot of different things. There are also several other documents that levy expectations on this organization and the NMEC director. This is a way to get my hands around these expectations, so we are trying to lay all that out and see how much of that is duplicative and overlapping. Then we will develop an implementation plan to find out what things we have done, what we are doing and prioritize what we need to start doing. We are laying that out right now, and the leadership team will work together to set priorities and make decisions on investment.

COMMUNIQUÉ: *Is there anything else that you would like to add?*

MR. MILLS: The mission here is really exciting, and it is clear how proud NMEC personnel are in working the mission and contributing in this way. Morale is very good here. I think when you realize where NMEC started and where it has come from, you see that it is really still a new organization. Roy Apseloff and the past and current leadership team get a lot of credit for growing and building NMEC into what it is and what it provides to our customers. ▲

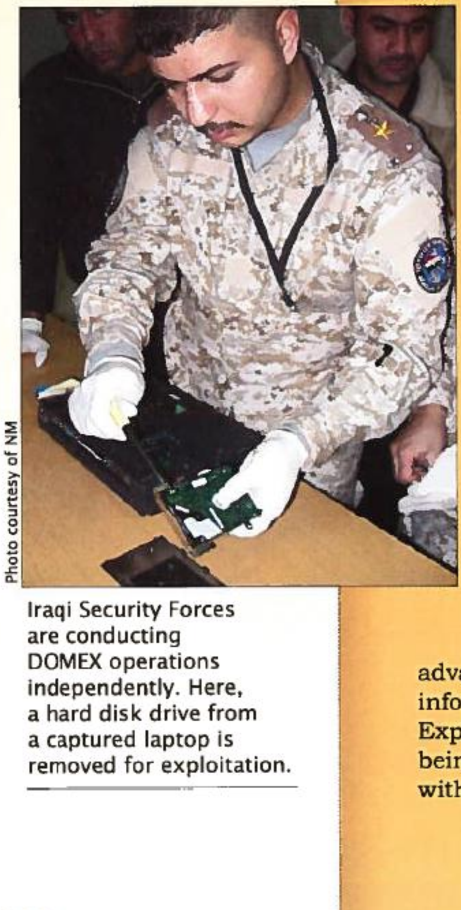


Photo courtesy of NM

Iraqi Security Forces are conducting DOMEX operations independently. Here, a hard disk drive from a captured laptop is removed for exploitation.

NEXSYS: The Next Generation Architecture

By Caryn D. Mercadante, NM

The National Exploitation System (NEXSYS) will make the challenge of handling and sharing document and media exploitation a thing of the past.

The National Media Exploitation Center's (NMEC's) ability to function as the national document and media exploitation (DOMEX) community hub is constrained by the existing information technology (IT) architecture. Currently there is no central repository to store DOMEX data, nor does the capability exist to remotely access and exploit raw DOMEX holdings. In response to their specific mission requirements, each DOMEX partner has developed their own solution to processing, storage and dissemination. Additionally, the ability to search and exchange data across different network domains is limited. This has resulted in uncoordinated efforts, duplicative storage and sharing impediments. Partners have forged numerous ad hoc arrangements in order to overcome the obstacles of an informal DOMEX system architecture.

NMEC is leading the development of a flexible and robust architecture to address the challenges of technological advancements, storage growth and information sharing. This National Exploitation System (NEXSYS) is being developed in coordination with DOMEX partners through the

NEXSYS Workgroup, which addresses the needs and equities of all partners and also solicits input from other interested parties within the DOMEX community. NEXSYS will incorporate a new family of systems that uses the best practices of legacy systems and capabilities while reducing redundancies. The NEXSYS Program Office is ensuring interoperability through the standardization efforts of the Intelligence Community Chief Information Officer's (CIO's) Integrated Information Oversight and Engineering (I2E) effort. Once fully funded and operational, NEXSYS will be capable of hosting specialized processing engines and tools from all partners.

In summary, NEXSYS tackles the following technical and operational challenges:

Community Cooperation. Fosters sharing, cooperation and coordination between members of the community in accordance with Intelligence Community Directive (ICD) 302.

- Facilitates interoperability of disparate systems forming a globally distributed and synchronized family of systems.
- Establishes, where necessary, and implements community standards:
  - In accordance with the Office of the Director of National Intelligence CIO's I2E, where appropriate.
  - Working with the Department of Defense and law enforcement for their comparable standards.
- Establishes a community-wide, centralized repository for sharing, storage, processing and life-cycle management of accumulated DOMEX data.

Sharing. Opens secure and safe access to the community's DOMEX holdings globally in accordance with the sharing principles within ICD 501.

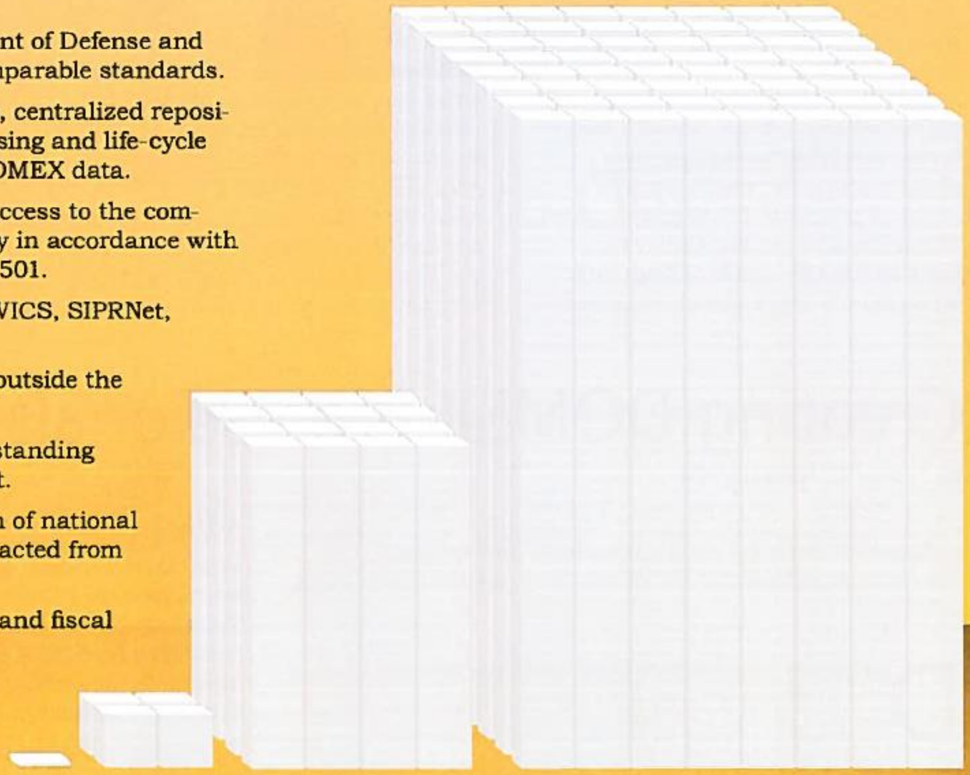
- Uses existing networks, e.g. JWICS, SIPRNet, NIPRNet and Stoneghost.
- Allows federated queries from outside the system to search DOMEX data.
- Provides automated profiling (standing queries) tailored to every analyst.
- Provides automated population of national databases with information extracted from DOMEX sources.

Efficiency. Increases operational and fiscal efficiency across the community.

- Improved productivity of limited resources through the automated synchronization of effort (knowledge of what each other is doing or has done).
- Consolidates geometric growth challenges to two sites instead of all sites.
- Consolidates DOMEX disaster recovery requirements to a single site.

Mission Accomplishment. Improves the community's ability to accomplish the mission and support global operations better and faster.

- Solves the storage and processing scalability issues.
- Decreases processing timelines from days to hours.
- Improves thoroughness and standardized processing results.
- Provides direct support and near real-time reachback from national to tactical, when connected.
- Standardizes and streamlines the process of integrating new exploitation capabilities. ▲


Megabyte (MB)
1 megabyte = 873 pages
Gigabyte (GB)
1 gigabyte = 894,784 pages
Terabyte (TB)
1 terabyte = 916,259,689 pages
Petabyte (PB)
1 petabyte = 938,249,922,368 pages

DOMEX Ops Keeps it REAL

By Colleen M. Foster, NM

Getting intelligence from acquired media quickly keeps the Document and Media Exploitation Division at NMEC on their toes.

The essence of National Media Exploitation Center (NMEC) operations is the Document and Media Exploitation (DOMEX) Division within the Office of Operations (Ops).

DOMEX Ops is charged with ensuring the rapid processing, exploitation, dissemination and reporting of all acquired and seized media within its holdings in order to enhance the safety and security of the nation. To accomplish this, DOMEX Ops keeps it REAL by providing "responsive exploitation always linked" to priorities for all media.

Photo by MSgt Jonathan Dott

SPC Arigna T. Kato collects sensitive materials, including a computer hard-drive, following the arrest of an Iraqi man for involvement with the manufacture of improvised explosive devises in the city of Dora in southern Baghdad, Iraq.

The first step in this process begins when the media arrives at the center, either electronically or physically. The media is quickly processed and uploaded into a local network where triage examiners and linguists rapidly scour the media for any items of potential intelligence value. These documents are then examined by another team of linguists who provide short gist summaries of the documents. Subsequently, at the customer's discretion, the digitized gist summaries are uploaded into the national Harmony database for access across the greater intelligence, law enforcement and homeland security communities. Lastly, NMEC stores a copy of the media, within the Common Data repository, so as new information is uncovered it can be compared and cross referenced against the historical data to identify new connections and linkages.

Throughout the exploitation process, teams of analytic liaisons from a wide range of intelligence community and DIA entities and offices, including counter improvised explosive devices, cyber threat, homeland security and counterterrorism, embedded at the center immediately begin examining these documents and media for information related to their specific areas of expertise. By working together, these analysts are able to identify and discover insights into how terrorists operate, enabling them to create timely, relevant, accurate and actionable intelligence that drives operations and foreign policy decision. NMEC customers, including national- and defense-level policy and decision-makers, commanders actively engaged in support of overseas contingency operations, and various law enforcement entities worldwide, demand responsive support in the form of technical exploitation and dissemination of information derived from captured media. DOMEX Ops is dedicated to providing this responsive exploitation of captured media to the customer and the community. ▲

Creating DOMEX Professionals

By Trevor G. Hassett, NM

Targeted training keeps document and media exploitation capabilities at the forefront in a war zone.

Document and media exploitation (DOMEX) requires a multifaceted array of technical, linguistic and managerial skills to deliver timely and effective support to combatant commands, law enforcement, homeland security and the intelligence community. The National Media Exploitation Center (NMEC) trains the cadre of DOMEX professionals assigned to a combined media processing center (CMPC) and a joint document exploitation center (JDEC). Currently, U.S. Central Command has a CMPC in Qatar and JDECs in Afghanistan and Iraq.

Volunteer civilians, service members and contractors learn how to provide DOMEX support from NMEC's Training Division, which is committed to providing quality instruction at DOMEX 101 and the NMEC Platform Leadership course to prepare deploying DIA and military service personnel in DOMEX roles.

All combatant commanders want exploitation capabilities at their fingertips, and the specific advantages offered by DOMEX include translations, digital media examinations, cellular phone exploitation and archival of all captured documents and media in a searchable database. Each unique skill set requires specialized training for not only the practitioners, but also the leaders that manage their

talents. As the demand for DOMEX increases exponentially, NMEC makes DOMEX training accessible to the entire intelligence community (IC).

Intelligence Community Directive 302 mandates that NMEC "develops and advocates programs, including training and tradecraft that expose all IC personnel to the benefits of using DOMEX activities and products and, in concert with other IC elements, trains IC personnel in DOMEX."

Currently NMEC offers virtual DOMEX training on SIPRNet and JWICS SharePoint portals. NMEC has expanded DOMEX offerings to the Joint Intelligence Virtual University (JIVU), including interactive learning and multimedia demonstrations of emerging technology. The NMEC Training Division promotes DOMEX by inserting realistic scenarios to numerous annual combatant command exercises.

Linguists working for NMEC receive professional development seminars on highly technical and scientific analytical topics. By familiarizing linguists with the specific vocabulary and key terminology used by analysts, they improve translations of foreign research documents and schematics.

A worldwide collection of these best practices shaped the current syllabus of courses offered through NMEC. Lessons learned from personnel returning from combat theaters are incorporated into a common standard for DOMEX operations. To meet the challenges of a rapidly evolving discipline, the NMEC Training Division continues to apply innovative, yet pragmatic approaches to maintain its status as the DOMEX center of excellence. ▲

Kristin Burke and Rick Hamby train Elysia Nuttall, currently on a DIA internship, the basic practices to extract data from a cellular phone.

Bringing DOMEX CAPABILITY to Our Coalition Partners

By Trevor G. Hassett, NM

The National Media Exploitation Center is bringing document and media exploitation training and technology to Iraq.

An assault team secures the objective and positively identifies the suspects targeted in the operation. They take all of the cell phones, pocket litter and electronic media found on site into custody and process it while the suspects are at the detention facility. Trained specialists exploit the contents of the phones, confirming connections to known members of al-Qaida in Iraq and identifying new targets for the next operation.

Although this scenario sounds familiar to anyone who has operated in Iraq over the last several years, this operation is unprecedented because every step is executed independently by the Iraqi Security Forces (ISF). With assistance from the National Media Exploitation Center (NMEC), the U.S. Forces-Iraq's (USF-I's) Iraq Training and Advisory Mission (ITAM) is teaching Iraqi soldiers and police how to conduct document and media exploitation (DOMEX). Twenty-first century technology is crucial to establishing security and promoting the rule of law in Iraq, and USF-I relies on the expertise of NMEC to select the right equipment and develop a DOMEX program of instruction.

In September 2009 NMEC enabled ITAM to offer DOMEX training at the Intelligence and Military Security School (IMSS) in Taji, Iraq. Since then, ITAM has taught more than 100 students and fielded dozens of basic DOMEX kits throughout the ISF. For the first time, Iraqi officers are exploiting documents, electronic media and cellular phones to support their operations.

IMSS leads the Iraqi Ministry of Defense training effort, and in March

2010 ITAM handed full responsibility of DOMEX instruction over to the faculty. The commandant of IMSS, Staff Brig. Gen. Abd al-Kaliq Salman, lauded DOMEX course graduates and their U.S. partners in the annual Military Day ceremony. The commandant said the DOMEX course curriculum represented a leap forward in the school's capacity to help the intelligence community fight terrorists and criminals in Iraq.

"Graduates form the nucleus of the new intelligence capability given to us by our U.S. allies, and I ask you to share information with your intelligence counterparts," he said in an English translation.

This spring the Ministry of Interior inaugurated DOMEX instruction at the National Investigation and Information Agency (NIIA) training center in Baghdad. According to Gen. Hadi Allami, director of technical affairs for NIIA, "The DOMEX teams give NIIA the ability to better exploit evidence collected from crime scenes and searches. Most importantly, this will help us solve more crimes and pre-empt future ones." ▲

Special thanks to SA Michael Milner and The Advisor, a USF-I publication.

LTC Muhammed Salman Ali of the IMSS faculty lectures DOMEX students on site exploitation.

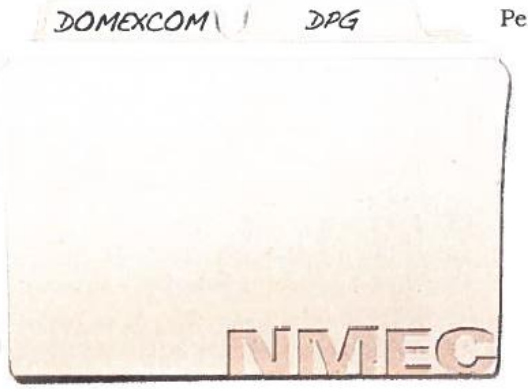
DOMEX Enterprise Governance and Doctrine

By Dave Barkley, NM

The Office of Policy and Doctrine brings organizations together to talk document and media exploitation.

The National Media and Exploitation Center's (NMEC's) Office of Policy and Doctrine (PD) serves as the principal coordinator for document and media exploitation (DOMEX) policy documentation development and dissemination, supports key intelligence community DOMEX activity discussions, is home to the NMEC briefing team, and has oversight of the NMEC continuity of operations (COOP) planning effort and remote site development.

The formation of NMEC raised the necessity of developing collaborative enterprises with other organizations engaged in DOMEX. Nurturing and strengthening these associations has required equitable, cross-community governance. NMEC PD provides this support through its coordination of the Office of the Director of National Intelligence (ODNI) DOMEX Committee (DOMEXCOM) activities, and one of its principal sub-groups, the DOMEX Policy Group (DPG). These fora encourage information sharing as well as critical DOMEX activity discussion affecting all of NMEC's partners. Key DOMEX community guidance is also developed, reviewed and approved via these groups.



Perhaps PD's most vital function is to ensure the availability of the most current DOMEX policy documentation and its compliance with best practices in cooperation with NMEC's partners. The most far-reaching aspect of this work has been the codification of content and formats for all DOMEX issuances being developed, updated or promulgated. The following major DOMEX activities are currently being pursued through this endeavor: an ODNI DOMEX classification guide, DOMEX community performance metrics and a revalidation of all intelligence community DOMEX issuances. Users can access this documentation as well as the full assortment of DOMEX policy documentation through a redesigned NMEC Policy and Doctrine website on JWICS at http://portal.nmec.ic.gov/sites/policy/_layouts/1033/viewlsts.aspx?BascTypc=1. NMEC is also providing subject matter expertise and working with the Office of the Undersecretary of Defense for Intelligence to establish a Department of Defense DOMEX directive that coordinates DOMEX activities in that key department.

The first and often only face of NMEC that visitors see is that of the visit itself and the briefing team. The team averages six briefings per week, each requiring extensive internal and external coordination to ensure that the audience's interests are being met and to develop round-table exchanges with appropriate NMEC operations, forensics, information technology and translation staffers. The onsite visits conclude with a walking tour of NMEC's extensive technology and linguistic resources, and frequently a courtesy call with NMEC's director. The team will also bring the NMEC

message to its customer; it conducts approximately 25 percent of its workload on the road.

NMEC PD is also developing the center's mission recovery plan for conducting COOP. The plan provides corporate guidance for CODE, or continuity of operations designation element, which are personnel who will relocate to NMEC's remote site in the event NMEC headquarters is unavailable. There they will execute NMEC's core mission-essential functions of media ingestion and exploitation, storage, dissemination and sharing.

A capsule characterization of NMEC PD's primary function might be its role as an air traffic controller of sorts — ensuring that a diverse group of federated partners are aware of each other's presence in overlapping activities; standardizing and deconflicting governing policy positions; availing a broad spectrum of customers with timely access to mission-critical data; and promoting cross-community awareness of DOMEX successes. ▲

UFAC DIGS DEEP to Find Covert Facilities

By the Underground Facility Analysis Center, DI

Have a target that resides hundreds of feet below the surface? The Underground Facility Analysis Center is here to help.

A graphic rendering of an underground facility.

Images courtesy of UFAC

The intelligence community is witnessing the re-emergence of an old warfighting domain — the subsurface domain — where underground facilities are used for offensive and defensive purposes. Where are our adversaries building their next underground uranium enrichment plant? How can we defeat an offensive ballistic missile site hidden hundreds of meters underground? These are some of the challenges the Underground Facility Analysis Center (UFAC) faces daily as nations are increasingly building deeper underground facilities to protect and conceal their most vital military capabilities, such as national leadership, military command and control, weapons of mass destruction and ballistic missiles. It is a difficult task to find covert underground facilities around the globe and determine their functions, operational status and vulnerabilities. This enormous task is the mission of UFAC.

UFAC is a government-wide consortium sponsored by the director of national intelligence (DNI) with DIA serving as the intelligence community's (IC's) executive agent. Experience has shown that no IC organization possesses all the requisite knowledge, skills and experience to tackle this daunting problem alone. Consequently, UFAC leads and manages a collaborative effort composed of intelligence and non-intelligence organizations, including subject matter experts from DIA, the National Geospatial-Intelligence Agency, the National Security Agency and the Defense Threat Reduction Agency.

Covert underground facilities can conceal a large array of capabilities.

UFAC's analysis provides vital information to U.S. policymakers, weapons developers and military forces and their commanders on how adversarial nations are using underground facilities for strategic advantage. New automated technologies to address adversarial underground facilities is one area the center is exploring to in response to the onslaught of underground construction. Recent advances in the use of automated algorithms have prioritized areas for further analysis. Additionally, continuing breakthroughs in underground facility characterization tools have improved combatant command crisis response time and reduced target intelligence uncertainty, leading to a higher probability of mission success.

To find out more about UFAC, go to their website at www.dia.ic.gov/admin/DI/web-content/Functional/UFAC.html. ▲

Cell Helps Bring Missing Service Members HOME

By the IC Prisoner of War/Missing In Action Analytic Cell, DI

This cell provides critical intelligence analysis to help bring missing service members and American citizens home.

History

On Oct. 11, 2000, Congress mandated the director of central intelligence "shall, in consultation with the Secretary of Defense, establish and maintain a POW/MIA intelligence analytic capability." The Intelligence Community (IC) POW/MIA Analytic Cell was established Sept. 18, 2001, to serve as the focal point for post-1990 prisoner of war/missing in action (POW/MIA) and personnel recovery-related all-source analysis within the IC.

In 2003 at the request of the Senate Select Committee for Intelligence, the cell's mission was expanded to provide intelligence support for the U.S. military service secretary status boards of inquiry. Additionally, in 2006 Department of Defense (DOD) Instruction 3115.10E, Intelligence Support to Personnel Recovery, was published that formally assigned hostage rescue intelligence responsibilities to the cell. The cell performs under the director of DIA's executive agent authorities and is assigned as a division within the Directorate for Analysis Joint Warfare Support Office (DI/JWS).

Missions and Functions

The POW/MIA Analytic Cell:

- Assesses plans, intentions, procedures and operations of state and non-state actors to capture or otherwise hold and exploit U.S. and allied personnel or their remains.
- Focuses appropriate and available analytic and collection resources on members of the armed forces and DOD civilians or contractors who, after Dec. 31, 1990, are unaccounted for.
- Produces baseline intelligence assessments on threats of capture, isolated persons, POW/MIAs, hostage events, personnel recovery, rescue and remains-recovery issues.
- Tasks, validates and provides intelligence oversight to worldwide POW/MIA and personnel recovery intelligence collection requirements.
- Surges to ensure timely and effective support to ongoing and future personnel recovery, POW/MIAs, and designated hostage and kidnap cases.
- Supports service secretary status boards of inquiry with the totality of all available national intelligence on missing or captured DOD persons.
- Conducts POW/MIA and personnel recovery liaison and fusion with the IC, combatant commands, military services, other DOD partners and U.S. allies.
- Develops appropriate personnel recovery, POW/MIA, and hostage and kidnap intelligence doctrine.
- Serves as the director of national intelligence's intelligence topic expert for the National Intelligence Priorities Framework POW/MIA topic.

In addition to working the recovery of live hostages, the cell with its IC partners and U.S. military, law enforcement and DOD medical counterparts, provides essential support in locating and recovering remains of post-1990 U.S. service members. On multiple occasions, analysts used advanced 3-D visualization, geospatial imagery and other analytic tools to assist the combatant commands in these recovery operations. From 2003 to 2009, this support contributed to the recovery of the remains of eight U.S. Army, Navy and Air Force personnel.

The IC POW/MIA Analytic Cell is committed to providing actionable, all-source analytic and collection POW/MIA and personnel recovery intelligence support to policymakers, planners, warfighters and U.S. allies.

> "The Intelligence Community (IC) POW/MIA Analytic Cell was established Sept. 18, 2001, to serve as the focal point for post-1990 prisoner of war/missing in action (POW/MIA) and personnel recovery-related all-source analysis within the IC."

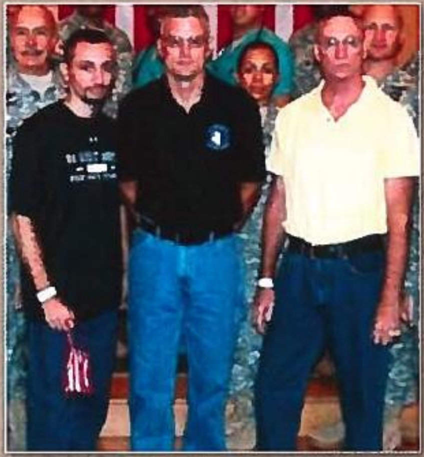
Cases

CAPT Michael Scott Speicher

◄ On Jan. 17, 1991, during Operation Desert Storm, CAPT Michael Scott Speicher was shot down over western Iraq by an Iraqi MiG-25. From October 2002 to August 2009, the cell led and coordinated the national analytic and collection efforts to account for him. The cell deployed analysts to the Iraq Survey Group in 2003 and 2004, and to the Multinational Forces – Iraq's Personnel Recovery Division from 2005 to 2009. These analysts and the cell's subject matter experts in Washington, D.C., provided dedicated analytic support. In July 2009, using the cell's analysis and information from a Bedouin tribesman, U.S. Marines recovered Speicher's remains.

On April 9, 2004, insurgents ambushed a U.S. Army convoy near Abu Ghurayb and captured SSG Keith Matthew Maupin. A video indicated he survived the attack. A second video showed the execution of an unidentified male. Using video enhancement technology and in-depth analysis, the cell assessed Maupin was the victim. ►

SSG Keith Matthew Maupin



From left to right: former FARC hostages Marc Gonsalves, Keith Stansell and Thomas Howes.

◄ From February 2003 to July 2008 the cell provided extensive support to the case of three DOD contractors captured by the Revolutionary Armed Forces of Colombia (FARC). The cell generated detailed analytic collection requirements and provided direct assistance to deployed forces, producing more than 100 intelligence products, briefs and assessments. On July 2, 2008, Colombian military forces rescued multiple hostages, including the three U.S. citizens.

Then President Bush welcomes two former Shelter Now International captives back to the U.S.

◄ During Operation Enduring Freedom, the cell provided intelligence that led to the rescue and recovery of the Shelter Now International aid workers detained in Kabul by the Taliban. The cell worked closely with its IC partners and allies to report information leading to this success.

▼ During Operation Iraqi Freedom, the cell provided 24/7 support to track, monitor and support all coalition POW/MIA events, isolated personnel, and combat search and rescue events. The cell's prewar analysis of Iraqi prisoner handling techniques and dedicated analytic and collection resources enabled them to provide critical intelligence in support of more than 50 personnel recovery events. Intelligence provided by the cell was key to the rescue of PFC Jessica Lynch.

PFC Jessica Lynch

The cell is currently engaged in supporting more than 40 U.S. and allied kidnapping cases by politically-motivated, anti-U.S. groups in Iraq, Afghanistan and other countries worldwide. Their assessments focus on the fate and disposition of these captives as well as providing detailed analysis on terrorist, insurgent and nation-state hostage taking tactics, techniques and procedures. ▼

SSG Ahmed Al-Taie

Timothy Bell

PFC Bowe Bergdahl

Photos courtesy of the POW/MIA Cell

Medical Intelligence Relies on TEAMWORK

By Damien K., NGA

The partnership between the National Geospatial-Intelligence Agency and the National Center for Medical Intelligence benefits not only DIA, but the intelligence community as a whole.

Comprehensive and significant geospatial intelligence (GEOINT) provided by the National Geospatial-Intelligence Agency (NGA) helps DIA's National Center for Medical Intelligence (NCMI) ensure successful mission completion.

"The partnership of NGA's imagery and geospatial intelligence analysts with NCMI's all-source intelligence analysts has created a model for an effective collaborative working relationship," according to Stephen J., deputy director of the NGA Support Team (NST) to DIA.

Applying imagery and geospatial analysis to medical intelligence has proved invaluable to NCMI, the Department of Defense (DOD) and the intelligence community (IC).

Medical intelligence includes the assessment of potential health risks and capabilities that allows planning for proper medical countermeasures and field health care for deployed forces. NCMI prepares and coordinates integrated, all-source intelligence for DOD and other government organizations on foreign health threats and other medical intelligence issues in support of U.S. interests worldwide.

For instance, NCMI's medical intelligence helps protect the health of forces deployed to Iraq and Afghanistan, as well as personnel stationed at home and throughout the world. NCMI analysts integrate multiple intelligence sources to enable decisions to prepare for, respond to and control health threats, particularly in situations where foreign countries do not report information to the press or international health organizations. NGA's GEOINT provides insight essential to this effort.

The NGA support team at NCMI includes experts in imagery and geospatial analysis who regularly engage with the center on three major focus areas: foreign military and civilian medical systems, environmental health risks and infectious disease risks. NGA collaborates directly and daily with NCMI analysts, from initial brainstorming on a problem to fine-tuning the final intelligence product.

"The in-house imagery analytical quality and content, and the unique geospatial data, analysis and tools NGA provides, are of paramount value and importance to NCMI and their customers," said Col Anthony Rizzo, director of NCMI.

NGA analysts work with NCMI's Environmental Health Division to produce environmental health intelligence reports such as industrial hazard assessments, industrial facility health risk assessments, and chemical and radiological hazard area models. Embedded NGA imagery analysts identify the locations and operations of facilities that could pose a physical or toxic health threat to U.S. forces operating in a specific area in the event of a catastrophic release. NGA geospatial analysts provide advanced analysis of geography and hydrology to predict the type, location and mobility of water contamination. These advanced analytic techniques greatly enhance the resolution and confidence of NCMI's assessments of potential health threats to U.S. forces overseas.

As an integral part of NCMI's effort to maintain the medical intelligence managed by its Medical Capabilities Division, NGA analysts help review a variety of source information used to locate medical facilities and assess healthcare infrastructures.

NCMI is routinely asked to recommend suitable healthcare facilities to treat U.S. personnel deployed overseas in the event of an emergency. "And that's where [NGA analysts] come in," said CDR David Davies, chief of NCMI's Medical Capabilities Division. "NGA analysts are often called upon to map locations and other nearby infrastructure."

Other areas requiring NGA's expertise include working with NCMI's Infectious Disease Division. Working with NCMI analysts, dedicated senior GEOINT analysts forecast, track and analyze the occurrence of infectious diseases with pandemic potential. The NGA role and mission in supporting the Infectious Disease Division dramatically increased during the 2009 H1N1 influenza pandemic.

"NGA's success in providing GEOINT to NCMI and the community during the first pandemic in 40 years was due to the mutual understanding, trust and cooperation developed between the two organizations over the last decade," according to Dr. Kathryn Morici, chief of NCMI's Infectious Disease Division.

In response to the potential human health threat posed by avian influenza, the NST established the GEOINT Pandemic Working Group in early 2008, about 16 months before the 2009 H1N1 pandemic emerged. Building on strong relationships through regular quarterly meetings and effective intra- and interagency

cooperation made the working group very effective within the GEOINT community before and during the pandemic.

The working group capped a successful 2009 by orchestrating the first NGA Pandemic GEOINT Conference with sessions in St. Louis and in Bethesda, Md., attended by representatives from throughout the government. Subject matter experts from the U.S. Department of Health and Human Services and the U.S. Centers for Disease Control and Prevention discussed the challenges with influenza surveillance and provided a basic understanding of the biology of the influenza virus.

The conference sessions identified and emphasized the value and utility of GEOINT tradecrafts as applied to pandemic risk mitigation and warning. Attendees also discussed the potential secondary and tertiary pandemic impacts on a global scale.

Whether planning a conference or providing GEOINT analysis, the bond between NGA and NCMI continues to grow. This extensive relationship benefits not only NCMI, but NGA partners in DOD, the intelligence community and elsewhere. ▲

Editor's note: Damien K. is chief of the NGA Support Team at the National Center for Medical Intelligence. This article is running concurrently in NGA's Pathfinder magazine.

LEADING EDGE:

UNLOCKING the Mystery of PKI

By Juanita L. Hairston, DS

Changes and upgrades to the DoDIIS Public Key Infrastructure are making the user's life easier and DIA more secure.

DoDIIS Public Key Infrastructure (PKI) on JWICS and NIPRNet are new and improved due to upgrades that facilitate broader usage of PKI for logging on to the network, e-mail encryption and signing, and Department of Defense PKI certificate-based authentication for Web servers.

The improvement and ease of PKI is a key focus of the Directorate for Information Management and Chief Information Officer (DS). You the user can benefit from PKI by reducing the number of passwords to memorize and creating a "single sign-on" experience across various technology applications. Simultaneously, the enterprise increases security by reducing the number of weak passwords.

On JWICS

A significant change to the PKI certificate process is the ability to enroll using either Internet Explorer, Mozilla Firefox, or Netscape on JWICS. Prior to this change, there were several DoDIIS sites that only supported Internet Explorer and did not have Netscape, which was required to download certificates. Consequently, the user would have to locate a workstation with Netscape or have it installed on the workstation. Now the enrollment process is much easier: You are able to use any of the three browsers supported by the enterprise, including Netscape, versions 4.7 through 7.2, and Internet Explorer, version 5.5 (SP1) and higher, to complete all activities within the PKI Certificate Management System.

The user experience has also been streamlined by enhanced automated functions on JWICS. PKI enrollment can be started using a name-based search as well as a user ID search, simplifying the process for users who do not know their new DoDIIS user ID. The enrollment process will no longer be sensitive to particular Web browser versions. Simply visit your local trusted agent with a valid picture ID, and your digital signature and key encipherment credentials will be e-mailed to you.

Step 1:
Check Eligibility for PKI Certificates

Verify that you are eligible to enroll for DoDIIS PKI certificates on the Certificate Management System page at https://pki.dodiis.ic.gov.

Step 2: Visit a trusted agent.

Visit your trusted agent, who will verify your identity and retrieve your enrollment pin. To locate a trusted agent, go to https://pki.dodiis.ic.gov and click "Trusted Agent Directory."

Step 3: Access your JWICS e-mail.

You will receive an e-mail with a link to initiate the identity verification.

Step 4: Download and execute the Intelligence Community Credential Wizard (ICCW).

You will receive a second and third e-mail with your certificates included, along with easy to follow installation instructions. Click on the first link in the "Enrollment Complete" e-mail to access the ICCW download page. Save "iccw.exe" to your H drive and launch the application.

With the new and improved enrollment process, it makes it easy to obtain PKI certification on JWICS by completing the four steps to the left.

After completing the four easy steps, you are now able to use your PKI certificate to send digitally signed or encrypted e-mails and access PKI-enabled applications and community of interest websites. PKI provides a world of innovative and exciting capabilities.

On NIPRNet

In addition to the changes on JWICS, Common

Access Card (CAC) readers have been deployed at NIPRNet workstations in the National Capital Region. This facilitates broader usage of PKI for network logon to NIPRNet. The CAC logon feature provides significant benefits, such as:

- More secure access to NIPRNet.
- Ability to digitally sign and encrypt e-mail messages on NIPRNet.
- Two options to log on to the DoDIIS.mil and DIA.mil domain on NIPRNet:
  - CAC and six- to eight-digit PIN.
  - Username and 14-character password requirement.

The 14-character password requirement to log on to the DoDIIS.mil and DIA.mil domains for NIPRNet access is mandated by the Joint Task Force – Global Network Operations. This requirement will go into effect in late April to early May 2010. Further guidance will be sent out to the work force regarding the date this change will take effect.

This change in logging on to the NIPRNet was not instituted to make your PKI experience challenging. As the user, you may favor the CAC reader and six- to eight-digit PIN login method. This is the preferred method, and the ultimate goal for all users logging on to NIPRNet. Logging on to NIPRNet with a CAC PIN will be fully functional when all user accounts are migrated from DIA.mil to DoDIIS.mil. Upon completion of the DoDIIS.mil migration on NIPRNet and with the significant enhancements using PKI and CAC, you will have an excellent user experience.

Don't delay! If you have not completed the PKI enrollment on JWICS and registered for a CAC to use on NIPRNet, do so today. Use of PKI provides many added benefits by allowing you to digitally sign and encrypt e-mail. It also reduces the number of passwords to remember by having a single sign-on across various technology applications. These benefits are enhancing the security of JWICS and NIPRNet by adding an additional layer of safety and protecting your computer data from unauthorized access, disclosure and modification.

Significant efforts are currently underway to provide security services and technology applications at all three network levels. Visit the DoDIIS PKI homepage at https://pki.dodiis.ic.gov for support and services and stay tuned for more information.

Photo by Eric J. Druxman, CS

▲ Kids got their blood pumping with a few jumping jacks during Take Your Child to Work Day.

Photo by Jonathon G. Schelmbauer, DI

◄ A Marine Corps volunteer demonstrates camouflage face paint techniques to Devon Cave, son of Judson Gallien, DI, during MSIC's Take Your Child to Work Day.

Photo by Eric J. Druxman, CS

▲ After demonstrating how to sniff out explosive material, Blue takes some time out of his busy schedule to accept his fans' adoration.

MSIC's LT Owen Schumaier explains how to use his gear. ▼

Photo by Michelle L. Henderson, DI

Photo by Eric J. Druxman, CS

▲ Tazman McPherson, left, and Tyeisha Hall, right, get a feel for weapons at the Chuckwagon demonstration.

TAKE
YOUR CHILD TO
WORK
DAY · APRIL 22

TJ, son of MSIC's Troy Carter is having a great time with one of the students from Columbia High School's JROTC Drill Team. ▼

Photo by Jonathon C. Schelmbauer, DI

Photo by Eric J. Druxman, CS

▲ Where's Blue?
Blue the explosives dog blends in with the children.

Photo by Donna C. Miller, DI

▲ President Abraham Lincoln tells a story to Jessica Miller, daughter of MSIC's Donna Miller.

Photo by Eric J. Druxman, CS

▲ Austin Landrum, left, and Andrew Young, right, review the agenda for events happening throughout the day at the DIAC.

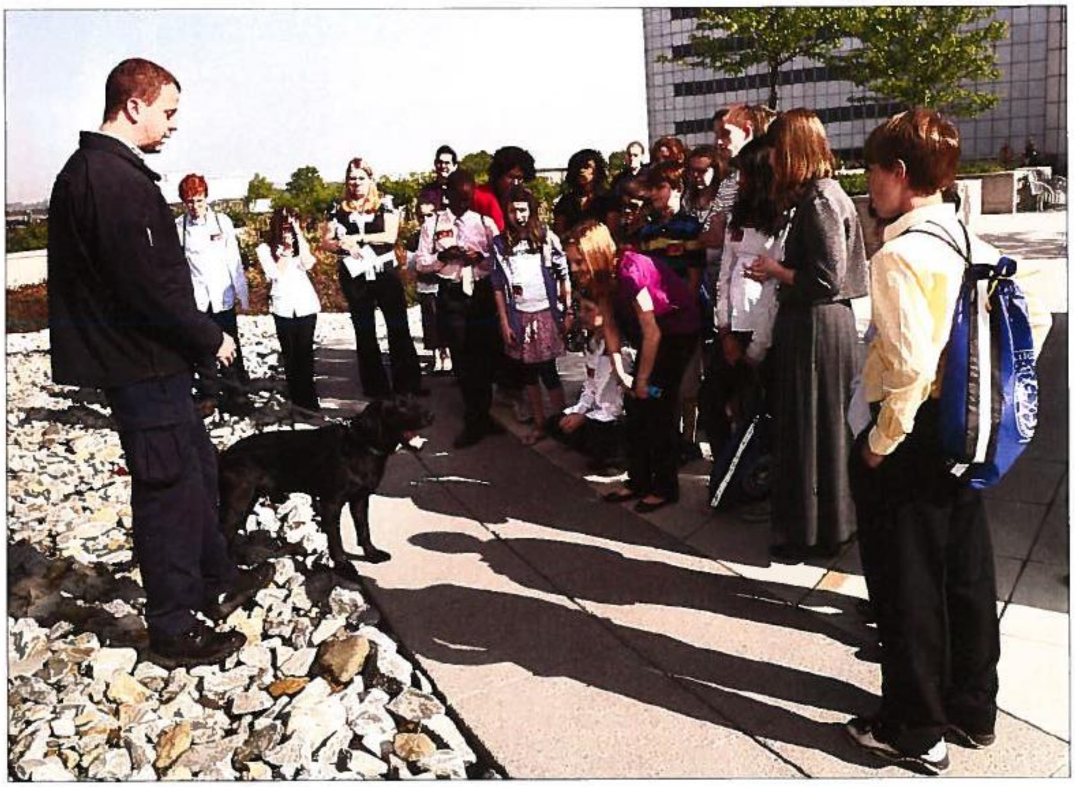
Photo by Eric J. Druxman, CS

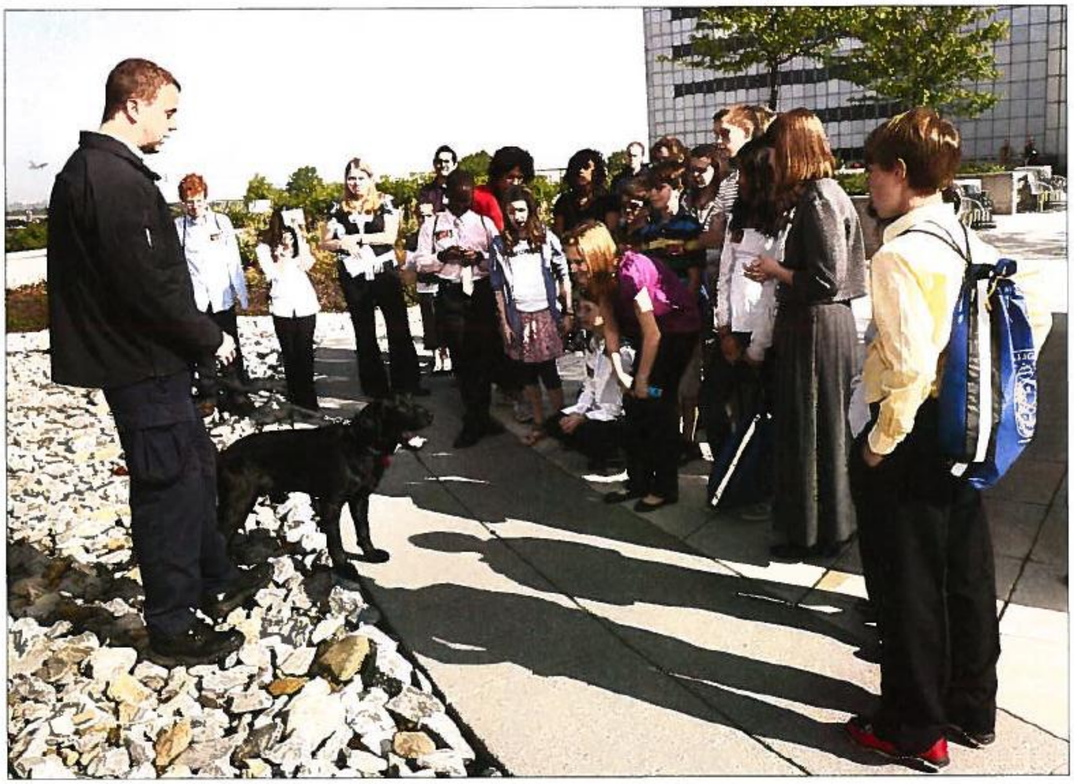
▲ LTG Ronald Burgess Jr., DIA director, talks with students from grades 8 to 12 during Take Your Child to Work Day.

Every Dog Has His Day

I spy with my little eye something ... furry.

During Take Your Child to Work Day at the DIAC, Blue demonstrated his superior explosives-sniffing techniques to a crowd of awe-struck children. After the exercise, however, the admiration of his skills turned into admiration of his adorable furry face. The bottom photo has been altered. The differences are subtle; can you find all 10 changes? The answers will run in the June 7 InterComm.





on the HORIZON

events for JUNE and JULY 2010

JUNE

National Safety Month

June 1 DX Ice Cream Social, 11 a.m., Crystal City

June 2 Operation Warfighter Initiative Luncheon and Career Fair for returning wounded warfighters and their families, 10 a.m. to 1:30 p.m., DIAC

June 3 Ice Cream Social, 11 a.m., TYCON 6

June 7-11 NSA's SIGINT Development Conference, Fort Meade, Md.

June 8 Ice Cream Social, 11 a.m., Crystal Park 5

June 9 DOD Asian Pacific American Leadership Forum and Workshop, noon to 4:30 p.m., Pentagon Conference Center

June 9 Costco table, 10 a.m., DIAC

June 9-10 Fancy Findings Vendor Fair, 9:30 a.m. to 1:30 p.m., Clarendon

June 10 DOD Asian Pacific American Leadership Forum and Workshop, 8 a.m. to 4 p.m., Double Tree Hotel, Crystal City, Va.

June 10 Costco table, 10 a.m., DIAC

June 10 Ice Cream Social, 11 a.m. to 1 p.m., DTT5

June 11 Costco table, 9:30 a.m. to 1:30 p.m., Clarendon

June 11 PNC Bank table 11, a.m. to 1 p.m., Clarendon

June 14 Army Birthday

June 14 Flag Day

June 14-18 DEOMI Special Emphasis Manager's Course, Holiday Inn, Huntsville, Ala.

June 15 Ice Cream Social, 11 a.m., Dulles North

June 15-16 DIA Enterprise Symposium, DIAC Lobby

June 15-16 In The Bag Vendor Fair, DIAC

June 17 HCH/HCL Supervisor Roundtable, 12:30 to 2:30 p.m., DIAC

June 17-18 In the Bag Vendor Fair, 9:30 a.m. to 1 p.m., Clarendon

June 20 Father's Day

June 21 First Day of Summer

June 22 In The Bag Vendor Fair, 9:30 a.m. to 2 p.m., Clarendon

June 22 Ice Cream Social, 11 a.m., Dorsey Park

June 23 Safety Day, DIAC

June 24 CWF Council Meeting, 9 a.m., DIAC

June 24-25 Sky Loom Vendor Fair, 9:30 a.m. to 1:30 p.m., Clarendon

June 25 Costco table, 9:30 a.m. to 1:30 p.m., Clarendon

June 29 Ice Cream Social, 11 a.m., DLOC

June 30 Ice Cream Social, 11 a.m., Pentagon

JULY

July 1 Pre Fourth of July Picnic, 11 a.m., DIAC

July 4 Independence Day (observed July 5)

July 6 Ice Cream Social, 11 a.m., Fort Detrick

July 7-8 Sparkling Ideas Vendor Fair, 9:30 a.m. to 1:30 p.m., Clarendon

July 8 Ice Cream Social, 11 a.m., Clarendon

July 9 Costco table, 9:30 a.m. to 1:30 p.m., Clarendon

July 13 DX Ice Cream Social, 11 a.m., Crystal City

July 13-14 HAS Sheet Sales, 10 a.m. to 2 p.m., DIAC

July 15 Ice Cream Social, 11 a.m., HIAC

July 15-16 HAS Sheet Sales, 9:30 a.m. to 2 p.m., Clarendon

July 19 Ice Cream Social, 11 a.m., TYCON 6

July 20-21 Jewelry Vendor Fair, 10 a.m., DIAC

July 21 MSIC Asian Pacific American Professional Development Seminar

July 21 HCH/HCL Supervisor Roundtable, 10 a.m. to noon, DIAC

July 22 CWF Council Meeting, 9a.m., DIAC

July 22-23 Sky Loom Vendor Fair, 9:30 a.m. - 1:30 p.m., Clarendon

July 23 Costco table, 9:30 a.m. to 1:30 p.m., Clarendon

July 23 PNC Bank table, 11 a.m. to 1 p.m., Clarendon

July 27 Ice Cream Social, 11 a.m., Crystal Park 5

July 29 Ice Cream Social, 11 a.m., Pentagon

For further information or updates concerning these events, please refer to the Internal Communications website.

DIA ENTERPRISE SYMPOSIUM

June 15 – 16, 2010

DIAC, Bolling AFB

Implementing the DIA Enterprise Vision

Integration of highly skilled intelligence professionals with leading edge technology to discover information and create knowledge that provides warning identifies opportunities, and delivers overwhelming advantage to our warfighters, defense planners, and defense and national security policymakers.

Learn more about the DIA Enterprise Symposium by visiting:

www.intelink.ic.gov/wiki/DIA_Enterprise_Symposium (JWICS)
www.intelink.sgov.gov/wiki/DIA_Enterprise_Symposium (SIPRNET)